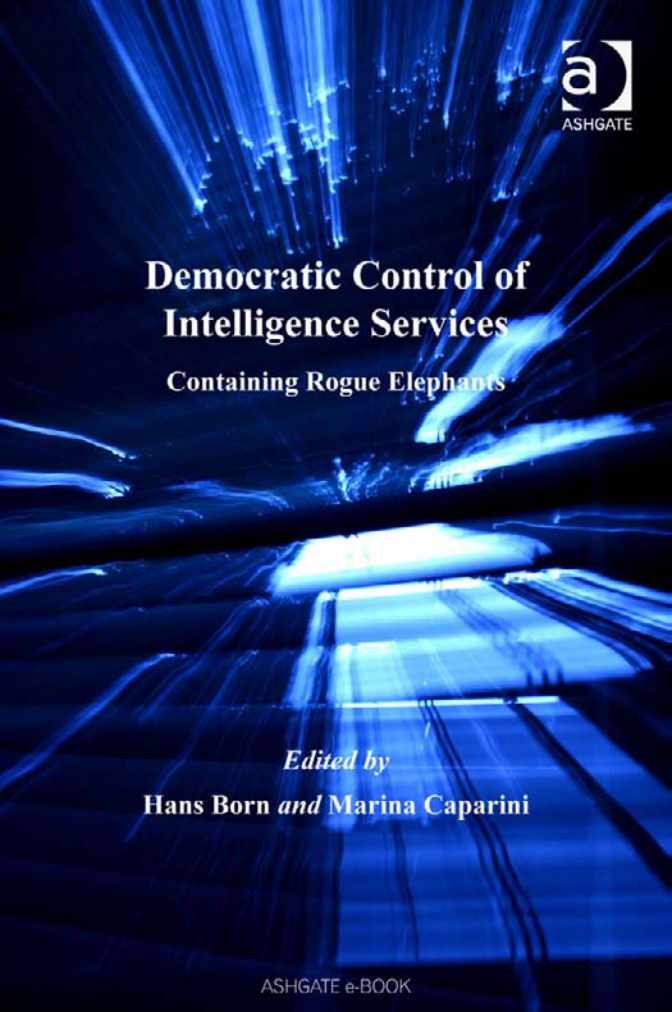

ASHGATE
Democratic Control of Intelligence Services
Containing Rogue Elephants
Edited by
Hans Born and Marina Caparini
ASHGATE e-BOOK

# DEMOCRATIC CONTROL OF INTELLIGENCE SERVICES

*This page intentionally left blank*

# Democratic Control of Intelligence Services

## Containing Rogue Elephants

*Edited by*

HANS BORN
*DCAF, Switzerland*
*and*
MARINA CAPARINI
*DCAF, Switzerland*

ASHGATE

Published by
Ashgate Publishing Limited
Gower House
Croft Road
Aldershot
Hampshire GU11 3HR
England

Ashgate Publishing Company
Suite 420
101 Cherry Street
Burlington, VT 05401-4405
USA

Ashgate website: http://www.ashgate.com

**British Library Cataloguing in Publication Data**
Democratic control of intelligence services : containing rogue elephants
1. Intelligence service - Management 2. Intelligence service - Government policy 3. Intelligence service - Political aspects
1. Born, H. (Hans), 1964- II. Caparini, Marina
353.1'7

**Library of Congress Cataloging-in-Publication Data**
Democratic control of intelligence services : containing rogue elephants / edited by Hans Born and Marina Caparini.
p. cm.
Includes bibliographical references and index.
ISBN: 978-0-7546-4273-2
1. Intelligence service--Management. 2. Secret service--Management. 3. National security. 4. Democracy. 5. World politics--1989- I. Born, H. (Hans), 1964- II. Caparini, Marina.
JF1525.I6D46 2007
353.1'7288--dc22

2006103134

ISBN: 978-0-7546-4273-2

Printed and bound in Great Britain by MPG Books Ltd, Bodmin, Cornwall.

# Contents

*This page intentionally left blank*

# List of Tables and Figure

*This page intentionally left blank*

# List of Contributors

**Mr David Banisar** is Deputy Director of Privacy International in London, the United Kingdom.

**Dr Hans Born** is Senior Fellow and Coordinator of the Working Group on Parliamentary Control of Armed Forces at the Geneva Centre for the Democratic Control of Armed Forces (DCAF) Geneva, Switzerland.

**Mr Nikolai Bozhilov** is Managing Director of the Centre for South East European Studies in Sofia, Bulgaria.

**Ms Marina Caparini** is Senior Fellow and Coordinator of the Working Group for Democratic Control of Internal Security Services, at the Democratic Control of Armed Forces (DCAF) Geneva, Switzerland.

**Mr Oldřich Černý** is Executive Director of Forum 2000 in Prague, the Czech Republic. He also served as National Security Advisor to the president of Czechoslovakia (1990–1993) and, as the first Director General of the Czech Foreign Intelligence Service (1993–1998).

**Prof. Peter Gill** is Professor in Politics and Security at John Moores University in Liverpool, the United Kingdom.

**Mr Hakon Huus-Hansen** is Head of the Secretariat of the Norwegian Parliamentary Intelligence Oversight Committee, Oslo, Norway.

**Ms Fairlie Jensen** is a Research Assistant at the Geneva Centre for Democratic Control of Armed Forces (DCAF) Geneva, Switzerland.

**Prof. Ian Leigh** is co-Director of the Human Rights Centre and Professor of Law at Law Department of Durham University, the United Kingdom.

**Mr George B. Lotz II** served as the Director of Policy, then as the Deputy and finally as the Assistant to the Secretary of Defense for Intelligence Oversight in the Office of the Secretary of Defense (1993–May 31, 2005) in Washington D.C, the United States.

**Dr László Majtényi** is Associate Professor of Law at Pecs University in Budapest, Hungary, and the former Hungarian Parliamentary Commissioner on Data Protection and Freedom of Information.

**Ambassador Leif Mevik** served as Chairman of the Committee for Monitoring of Intelligence, Surveillance and Security Services of Norway (1999–2006).

**Mr Fred Schreier** is a Senior Consultant for Research at the Geneva Centre for the Democratic Control of Armed Forces (DCAF) Geneva, Switzerland.

**Dr Larry L. Watts** served as Consultant to the Office of the National Security Advisor of the Romanian President in Bucharest, Romania.

**Ambassador Theodor H. Winkler** is the Director of the Geneva Centre for the Democratic Control of Armed Forces (DCAF) Geneva, Switzerland.

**Mr Thorsten Wetzling** is a doctoral candidate at the Geneva Graduate Institute of International Studies (IUHEI) where he also teaches seminars in political science and international organisation.

**Prof. Andrzej Zybertowicz** is Director of the Institute of Sociology, Nicholas Copernicus University in Torun, Poland.

# Preface

*Ambassador Theodor H. Winkler*

Intelligence services play a crucial role in democracies. Without timely and adequate intelligence, democracies would be more vulnerable to various threats, be they military, political or economic threats, both domestic and external threats. Notably after the terrorist attacks of 9/11 as well as numerous other major terrorism attacks in, for example, Bali (2002 and 2005), Moscow (2002), Casablanca (2003), Beslan (2004), Madrid (2004), London (2005), New Delhi (2005) and Mumbai (2006), it became widely acknowledged that intelligence services are indispensable; that they need to perform and coordinate better; and, that they need to have special powers and maintain secrecy of their operations in order to be effective. Yet at the same time, it is equally widely acknowledged that the special powers and secrecy of intelligence services can also be abused and may lead to unauthorised and illegal actions as well as inefficiencies or even – as widely charged in the US and the UK after the Iraq war – the politicisation of intelligence services. Finding the right balance between civil liberties and the protection of national security is a major challenge faced by all democracies. In this context it needs to be underlined that civil liberties and national security are not at odds with each other but that human rights and fundamental freedoms contribute to security – especially if one takes the position that security means the protection of the fundamental values of a society against any possible threat.

To date, very little international comparison of democratic accountability of intelligence services has been carried out, in particular with regards to the role of the executive and parliament as well as other independent oversight institutions. With the support of the Geneva Centre for the Democratic Control of Armed Forces, this volume tries to fill the gap and to contribute to the international exchange of ideas, approaches and practices related to the accountability of intelligence services. Doing so, this volume hopes to inform a substantive debate among lawmakers, government officials, intelligence officials as well as human rights activists, independent experts and journalists about the oversight and role of intelligence services in democratic societies.

*This page intentionally left blank*

# Acknowledgements

The idea for this book has its origins in discussions at the Geneva Centre for the Democratic Control of Armed Forces (DCAF) on new challenges for the democratic control of intelligence services in both 'new' and 'mature' democracies in the post-Cold War and post-9/11 era. These discussions have lead to a DCAF Research Department publication project on the role of oversight institutions in maintaining control and accountability of intelligence services as well as helping to ensure that they act within the rule of law. The project was initiated in 2002 in cooperation with noted international experts, including the contributors of this book. We wish to thank the contributors for their chapters and for the updating which several of them undertook as late as summer 2005, since some delays were encountered during the preparation of this volume.

A number of debts have been incurred in the implementation of this project and we would like to acknowledge them here. Ingrid Beutler, Michael Jaxa-Chamiec, Fairlie Jensen, Jason Powers, Wendy Robinson, Vincenza Scherrer, Aidan Wills and Camila Vega provided invaluable administrative, organisational and editorial assistance in the course of this project. We are also grateful to the anonymous reviewers of Ashgate Publishers for providing us with a number of incisive comments and useful suggestions on earlier drafts of the manuscript or parts thereof. Kirstin Howgate, Carolyn Court and Pauline Beavers at Ashgate Publishers steered us through the publication process with patience and encouragement. We would like to thank all of them and to express our special gratitude to the contributors of this book who did a wonderful job in meeting the demands the editors made on them.

Hans Born and Marina Caparini
Geneva, December 2006

*This page intentionally left blank*

# List of Acronyms

| | |
|---|---|
| ABW | *Agencja Bezpieczeństwa Wewnętrznego* (Agency for Internal Security), Poland |
| AIVD | *Algemene Inlichtingen- en VeiligheidsDienst* (General Information and Security Service), the Netherlands |
| AN | *Alianța Națională* (National Alliance, Romania) |
| APADOR-CH | *Asociația Pentru Apărarea Drepturilor Omului în România – Comitetul Helsinki* (Romanian Helsinki Committee), Romania |
| ASIO | Australian Security Intelligence Organisation |
| ASIS | Australian Secret Intelligence Service |
| ATIA | Access To Information Act, Canada |
| ATSD (IO) | Assistant to the Secretary of Defence for Intelligence Oversight, US |
| AW | *Agencja Wywiadu* (Foreign Intelligence Agency), Poland |
| BBC | British Broadcasting Corporation |
| BIS | *Bezpečnostní informační služba* (Information Security Service), Czech Republic |
| BOR | *Biuro Ochrony Rządu* (Bureau for Protection of the Government), Poland |
| BRGE | *Brigade de Renseignement et de Guerre Electronique* (Intelligence and Electronic Warfare Brigade), France |
| BSP | *Bălgarska Socialističeska Partija (* Bulgarian Socialist Party) |
| CBFOC | Central Bureau for Fighting Organised Crime, Bulgaria |
| CCSDN | *Commission Consultative du Secret de la Défense Nationale*, (Advisory Commission on National Defence Secrets), France |
| CFPDS | *Komisia po vanshna politika, otbrana i sigurnost* (Parliamentary Commission for Foreign Policy, Defence and Security), Bulgaria |
| CFSN | *Consiliul Frontului Salvării Naționale* (Council of the National Salvation Front), Romania |
| CID | *Centro Nacional de Inteligencia* (National Intelligence Centre), Spain |
| CNCIS | *Commission Nationale de Contrôle des Interceptions de Sécurité* (National Commission for the Control of Security Interceptions), France |
| CI | counter-intelligence |
| CIA | Central Intelligence Agency, US. |
| CIPA | Classified Information Protection Act, Bulgaria |
| CIR | *Comité Interministériel de Renseignement*, (Interministerial Committee for Intelligence), France |
| CNIL | *Commission Nationale de l'Informatique et des Libertés*, (National Commission for Freedom of Information), France |

| | |
|---|---|
| CNSAS | *Consiliul Național pentru Studierea Arhivelor Securității* (National Council for the Study of the Securitate Archives), Romania |
| CNSS | Center for National Security Studies |
| CPUN | *Consiliul Provizoriu de Uniune Națională* (Provisionary Council for National Unity), Romania |
| CRS | *Compagnies Républicaines de Sécurité*, (Companies for Republican Security), France |
| CSAT | *Consiliul Suprem de Apărare al Țării* (Supreme Defence Council of the Country), Romania |
| CSI | *Conseil de Sécurité Intérieure*, (Council of Interior Security) France |
| CSIS | Canadian Security Intelligence Service |
| DIA | Defence Intelligence Agency |
| DCAF | Geneva Centre for the Democratic Control of Armed Forces |
| DCI | Director of Central Intelligence, US |
| DCPJ | *Direction Centrale de la Police Judiciaire,* (Judicial Police), France |
| DCRG | *Direction Centrale Renseignement Généraux,* (Central Directorate of General Intelligence), France |
| DCSSI | *Direction Centrale de la Sécurité des Systèmes d'Information*, (Central Directorate for Security of Information), France |
| DDCI | Deputy Director of Central Intelligence |
| DGIA | *Direcția Generală de Informații al Apărării* (General Directorate of Defence Intelligence of the Defence Ministry), Romania |
| DGIPI | *Direcția Generală de Informații și Protecție Internă* (General Directorate of Intelligence and Internal Protection), Romania |
| DGPA | *Direcția Generală de Protecție și Anticorupție* (General Directorate for Protection and Anti-Corruption), Romania |
| DGPN | *Direction Générale de la Police Nationale* (National Police) , France |
| DGSE | *Direction Générale de la Sécurité Extérieure*, (Foreign Intelligence Agency), France |
| DHS | Department of Homeland Security, US |
| DIRC | Defense Investigative Review Council, US |
| DIS | Defence Information Service, Bulgaria |
| DIS | Defence Intelligence Staff, UK |
| DNI | Director of National Intelligence, US |
| DoD | Department of Defense, US |
| DOJ | Department of Justice, US |
| DP&FOIA | Törvény a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról (Data Protection and Freedom of Information Act), Hungary |
| DPSD | *Direction de la Protection et de la Sécurité de la Défense*, (Directorate for Defence Protection and Security), France |
| DRM | *Direction du Renseignement Militaire,* France |

| | |
|---|---|
| DSD | Defence Signals Directorate, Australia |
| DST | *Direction de la Surveillance du Territoire*, France |
| ECHR | European Convention on Human Rights |
| ECtHR | European Court of Human Rights |
| EO | Executive Order, US |
| EOS | *Etteretnings-, overvåkings- og sikkerhetstjeneste* (Intelligence, Surveillance and Security Services), Norway |
| EPIC | Electronic Privacy Information Center, UK |
| EU | European Union |
| FAC | Foreign Affairs Committee, UK |
| FBI | Federal Bureau of Investigation, US |
| FBIS | *Federální bezpečnostní a informační služba* (Federal Security Information Service), Czech Republic |
| FISA | Foreign Intelligence Surveillance Act, US |
| FO/E | Headquarters Defence Command Norway/Intelligence Division |
| FOI | Freedom of Information |
| FOZZ | *Fundusz Obsługi Zadłużenia Zagranicznego* (Foreign Debt Service Fund), Poland |
| GCHQ | Government Communications Headquarters, UK |
| GDR | German Democratic Republic |
| HC | House of Commons, UK |
| HEJP | *Institut des Hautes Etudes sur la Justice*, (Graduate Institute of Legal Studies), France |
| HNSC | *Academia Națională de Apărare* (Higher National Security College), Romania |
| HUMINT | Human Intelligence |
| IFJ | International Federation of Journalists |
| IG | Inspector General |
| IGI | Inspector General for Intelligence, US |
| IOB | Intelligence Oversight Board, US |
| IRS | Internal Revenue Service, US |
| ISA | Intelligence Services Act, UK |
| ISC | Intelligence and Security Committee, UK |
| ISMB | *Inspectoratul de Securitate al Municipiului București* (Inspectorate for the Municipality of Bucharest), Romania |
| ITT | International Telephone and Telegraph Company |
| JIC | Joint Intelligence Committee, UK |
| JTAC | Joint Terrorism Analysis Centre, UK |
| KGB | *Komitet Gosudarstvennoy Bezopasnosti* (Committee for State Security), Soviet Union |
| MAP | Membership Action Plan (NATO) |
| MI5 | Security Service, UK |
| MI6 | Secret Intelligence Service, UK |
| MİT | *Milli İstihbarat Teşkilatı* (National Intelligence Organisation), Turkey |

| | |
|---|---|
| MND | *Ministerul Apărării Naționale* (Ministry of National Defense), Romania |
| MoI | Ministry of the Interior, UK |
| MoD | Ministry of Defence, UK |
| MP | Member of Parliament |
| NATO | North Atlantic Treaty Organisation |
| NATO-MAP | North Atlantic Treaty Organisation - Member Action Plan |
| NCTC | National Counterterrorism Center, US |
| NGO | Non-governmental Organisation |
| NII | *Serviciul Național de Informații* (National Intelligence Institute), Romania |
| NIS | *Nacionalna Razuznavatelna Sluzhba* (National Intelligence Service), Bulgaria |
| NoNSA | Norwegian National Security Authority; Norway |
| NPS | National Protection Service, Bulgaria |
| NSA | National Security Agency, US |
| NSAC | National Security Advisory Council, Bulgaria |
| NSS | National Security Service, Bulgaria |
| NZZ | *Neue Zürcher Zeitung* (Swiss newspaper) |
| OAS | Organisation of American States |
| OPCD | *Úřad pro ochranu ústavy a demokracie* (The Office for the Protection of Constitution and Democracy), Czech Republic |
| OSPAR | Convention for the Protection of the Marine Environment of the North-East Atlantic |
| PAIA | Promotion of Access to Information Act, South Africa |
| PFIAB | President's Foreign Intelligence Advisory Board, US |
| PM | Prime Minister, UK |
| PNA | *Procuratura Națională Anticorupție* (National Anti-Corruption Prosecutor's Office), Romania |
| PNL | *Partidul Național Liberal* (National Liberal Party), Romania |
| PNTCD | *Partidul Național Țărănesc - Creștin Democrat* (National Peasant Party Christian Democratic), Romania |
| Q&A | Questions and Answers |
| RADET | Regia Autonoma de Distributie a Energiei Termice Bucaresti, Romania |
| RAM | Revolutionary Action Movement, US |
| RCMP | Royal Canadian Mounted Police Security Service, Canada |
| RIPA | Regulation of Investigatory Powers Act, UK |
| SB | *Służba Bezpieczeństwa* (Security Service), Poland |
| SCIS | State Commission on Information Security, Bulgaria |
| SDECE | *Service de Documentation Exterieure et de Contre-espionage*, France |
| SDS | *Sajoz na Dcmoknatichnite Sili* (Union of Democratic Forces), Bulgaria |
| SGDN | *Secrétariat Général de la Défense Nationale*, France |
| SIAC | Special Immigration Appeals Commission, UK |

| | |
|---|---|
| SIE | *Serviciul de informații externe* (foreign intelligence), Romania |
| SIGINT | Signal intelligence |
| SIPA | *Serviciul Independent de Protecție și Anticorupție* (The Independent Protection and Anti-Corruption Service), Romania |
| SIRC | Security Intelligence Review Committee, Canada |
| SIS | Secret Intelligence Service, UK |
| SISMI | *Servizio per le Informazioni e la Sicurezza Militare* (Italian Military Intelligence Service), Italy |
| SNI | *Serviço Nacional de Informações* (National Intelligence Service), Brazil |
| SPP | *Serviciul de Pază și Protecție* (The Guard and Protection Service), Romania |
| SRI | *Serviciul Român de Informații* (Domestic Security Intelligence), Romania |
| SRO | State Records Office, Bulgaria |
| SSCI | Senate Select Committee on Intelligence, US |
| STASI | Ministerium Für Staatssicherheit (Ministry for State Security), former German Democratic Republic |
| STB | *Státní Bezbečnost* (Communist Police), Czechoslovakia |
| STHS | Subcommittee on Terrorism and Homeland Security, US |
| STS | *Serviciul de Telecomunicații Speciale* (Special Telecommunications Service), Romania |
| TECHINT | Technical intelligence |
| TTIC | Terrorist Threat Integration Centre, US |
| UK | United Kingdom |
| UM | *Unitatea Militară al Ministeriului de Interne* (The Interior Ministry's Military Unit), Romania |
| UN | United Nations |
| UNDP | United Nations Development Programme |
| UOP | *Urząd Ochrony Państwa* (Civilian Office of State Protection), Poland |
| ÚSZI | *Úřad pro zahraniční styky a informace* (Office for Foreign Relations and Information), Czech Republic |
| VIP | Very Important Person |
| VOZ | *Vojenské obranné zpravodajství* (Military Defence Intelligence), Czech Republic |
| WMD | Weapons of Mass Destruction |
| WSI | *Wojskowe Służby Informacyjne* (Military Information Services), Poland |
| WTO | World Trade Organisation |
| ZSGŠ | *Zpravodajská služba generálního štábu* (Intelligence Service of the General Staff), Czech Republic |

*This page intentionally left blank*

# PART I

# Introduction

*This page intentionally left blank*

Chapter 1

# Controlling and Overseeing Intelligence Services in Democratic States

*Marina Caparini*

## Introduction

Intelligence and security services are key components of any state, providing independent analysis of information relevant to the external and internal security of state and society and the protection of vital national interests. A fundamental precept of democratic theory is securing and maintaining public consent for the activities of the state. Consequently intelligence agencies must be perceived as performing a necessary function, operating efficiently and effectively, accountable for their actions and those of their members, and under the firm control of elected authorities. As with any other public sector activity, citizens of democratic countries should expect effectiveness, efficiency, sound management and good value for money from the state's intelligence sector.

However the intelligence sector is also a special area of state activity. It has a vital role in safeguarding national security (and in some extreme cases, the survival of the state), resulting in a strong imperative for secrecy. Yet, if not subject to control and oversight, the intelligence sector's unique characteristics – expertise in surveillance, capacity to carry out covert operations, control of sensitive information, and functioning behind a veil of secrecy – may serve to undermine democratic governance and the fundamental rights and liberties of citizens. Special challenges arise in terms of establishing effective oversight mechanisms of this sector, which, next to the armed forces, has greatest potential to affect the political life of the nation. Democratic societies need to ensure that intelligence and security services do not influence or interfere in party political competition. Although maintaining effective control and oversight over the intelligence community is as important to the democratic vitality of a polity as maintaining control over the armed forces, intelligence services have received much less attention from scholars and those supporting democratisation processes.

The challenge of control and oversight of intelligence has also been framed in terms of the relative value placed on the community's collective need for security on the one hand, and individual rights and freedoms on the other hand. For example, revelations in late 2005 that President George W. Bush had authorised secret eavesdropping on telephone calls and emails of US citizens, bypassing the

requirement for warrants required by the Foreign Intelligence Surveillance Act (FISA) and the Fourth Amendment of the US Constitution, and more recent disclosures about the Federal Bureau of Investigation (FBI) authority to issue National Security Letters ordering certain types of business to turn over sensitive customer records, have provoked accusations that surveillance under the Bush is free from traditional legal constraints (Pitts, 2007). The question that arises is whether protecting the security of the state should trump all other objectives and values within society – that is, whether security represents an 'absolute value', which would then preclude any constraints on it (Hastedt, 1991a, p. 10). While national security is a legitimate and primary concern of any state, democratic states – and especially the liberal democratic variety – define themselves by the importance they place on democratic values, human rights and civil liberties. Accordingly, they must strive to observe and uphold these values to the greatest extent possible. Security is one value amongst many, and must coexist and compete with other values in the calculus that society conducts by means of its elected government to allocate scarce resources. In a liberal democratic state, security intelligence must exist 'within the context of respect for civil rights, free speech, the rule of law, checks and balances or other values held to be important by society' (Hastedt, 1991a, p.10). The quest of intelligence control and oversight in the democratic state, then, is to enable agencies to produce effective security intelligence while ensuring that they operate within the law and in a way that is consistent with democratic norms and standards.

This volume approaches intelligence and intelligence agencies with a primary focus on democratic oversight, underlining the challenges of holding to account those who operate in an area of activity in which secrecy and discretion constitute essential components. The argument of this chapter is that security and intelligence agencies have special requirements and features that make effective oversight particularly challenging, even in the most 'mature' democratic systems. It begins by considering what is intelligence and looks more closely at the relationship between policy and intelligence, and therefore at the governance or control by the executive of intelligence as a public policy sector. It then sketches the main mechanisms of control and oversight, turning to focus more closely on structural problems inherent in intelligence oversight. It ends by noting the challenges in intelligence governance and oversight faced by post-communist regimes, and identifies some issues raised by 9/11 and other recent trends concerning security intelligence.

## What is Intelligence?

Intelligence refers to 'information relevant to a government's formulating and implementing policy to further its national security interests and to deal with threats to those interests from actual or potential adversaries' (Shulsky, 2002, p. 1). It also refers to the activity and process by which information is systematically collected and made available to government officials in a usable form. The intelligence 'product' is composed of analyses and assessments, including raw

data. In sum, the term intelligence encapsulates a broad range of activities and all have the obtaining of or denying of information in common.

Intelligence, then, is the collection and analysis of information, presented to policy-makers in a form that will help them in their decision-making process and their choice of policy options. Intelligence can be directed externally towards foreign entities such as other states and non-state actors. It can also be directed against perceived domestic threats to the security of the state and society, which is traditionally known as security or security intelligence. Received wisdom holds that modern democratic states delineate between internal and external security intelligence with separate services. It should be noted, however, that with globalisation, the emergence of the threat of international terrorism, and state responses to that perceived threat, the distinction between external and internal is increasingly questioned, as demonstrated by the erosion of the institutional firewalls that were earlier erected between intelligence and security agencies.

Within government, intelligence has come to be thought of as comprising four main activities: collection, analysis and estimates, counterintelligence and covert action. Counterintelligence (see below) concerns information or activities aimed at neutralising the activities of hostile intelligence services and are necessary to protect the state's secrets from falling into the hands of other states. Covert action is an activity which is aimed to influence foreign governments while keeping the sponsoring government's involvement of the operation a secret.

Covert action (also known as active missions or direct action) has been said to offer a 'third option', or an alternative form of action to states between the polarities of diplomacy on the one hand, and the application of military force through war on the other. If a country chooses to endow its intelligence service with this function, the service moves beyond collecting and analysing information. It may, for instance, involve attempts to cause a change in regime, provision of political advice, financial support, technical assistance, propaganda, private training of individuals, economic and paramilitary activities, or even assassinations. Part of its attraction to the executives of certain democratic states may well lie in it being largely beyond the scope of legislative oversight (Johnson, 1989, p. 60). Covert action has recently attracted more attention because of the nature of issues on the international agenda of major Western states, particularly the threat of international terrorism and internal political change (democratisation) in formerly authoritarian states. Nevertheless covert action remains a highly controversial subject, and some American observers maintain that it has done more damage to the US reputation than helped achieve its foreign policy objectives, even during the Cold War (Hilsman, 1995, pp. 104–116).

## Counterintelligence and Security Intelligence Apparatuses

Counterintelligence activities and security intelligence about other threats to internal security impact most directly on the state of democracy and the fundamental freedoms and liberties of citizens, and this tends to be where most of the problems and controversies arise. Counterintelligence is aimed at countering

the actions of hostile intelligence services. Internal or domestic security has a broader focus than counterintelligence. Traditionally it concerns providing protection from coercive and clandestine efforts by foreign actors to advance their interests within a country by means such as espionage, terrorism or sabotage. Internal security has also been concerned with providing protection against subversion, or actions which are intended to overthrow or undermine parliamentary democracy by political, industrial or violent means, and other actions by domestic actors to undermine democracy, through organised crime for instance.

Intelligence services of totalitarian and authoritarian regimes have typically been targeted internally towards perceived political opponents and critics of the party, government or regime. Noteworthy examples from the former state socialist regimes in Central and Eastern Europe include the KGB in the former Soviet Union, the *Stasi* in former German Democratic Republic, and the *Securitate* in Romania. Those security services have gained a measure of infamy for their repressive activities, penetration of many spheres of social activity, and systematic abuse of human rights against citizens of the state concerned.

In principle, democratic states seek to constrain the activities of intelligence services against their own citizens, and ensure they do not overstep their legal and ethical boundaries. However, democratic states have also been known to target persons posing alleged and perceived threats to internal stability and security such as the members of the Black civil rights movement and anti-Vietnam war protesters in the US, as well as Communist Party members, union leaders and political and disarmament activists in numerous western states during the Cold War.

It is thus vital to know under what conditions a government agency can legitimately conduct surveillance of a citizen. There are two approaches to this question: The predominant approach has been to focus on the means of domestic intelligence – that is, the procedures for authorising wiretaps, searches, and surveillance. For example, in the US, the Church Committee attempted to apply the 'criminal standard' to domestic intelligence, limiting domestic intelligence investigations to those situations where a violation of law has occurred or is about to occur. The US adopted the criminal standard after the Church Committee found that there were many instances when the FBI was instructed by the White House to investigate political opponents of the President.

The other approach to domestic intelligence is to ask what the proper objective of such surveillance in a democracy should be (Shulsky, 2002, p. 148). That is, what are the threats that are driving domestic intelligence activities, and to what extent are individuals or groups who are engaged in legal activities subject to surveillance? While totalitarian and authoritarian regimes have been notorious for using intelligence and security agencies against opponents to the political leadership and regime, democratic states are supposed to protect freedom of speech, opinion, assembly, political opposition, political protest and dissent unless they threaten violence, national security, or the overthrow of the government. It is consequently of utmost importance in a democracy to delineate those conditions under which a state limits those fundamental rights and liberties of its citizens.

Security intelligence services have the potential to harm those very people whom they are designed to protect: citizens, who may have questioned or challenged specific policies and decisions of the government in power. In liberal democracies, the right of citizens to voice dissent from their governments' policies is highly valued as the mark of a free society. Awareness that they may be subject to surveillance and monitoring because of their involvement in controversial public activity or organisations, and even more so the possibility that they may suffer monetary and career setbacks from being labelled a 'security risk' may lead people to limit or abstain from such activity. This is known as the 'chilling effect', and it exerts a negative influence on social activism, free expression and public discourse (Hannant, 2000, pp. 214, 218).

## Policy-Relevant and Policy-Neutral Intelligence

There is a certain tension that is evident in the relationship between intelligence and policy (specifically between intelligence services and the executive), and the relationship between them is also subject to disagreement among scholars and practitioners. While intelligence is supposed to help answer questions for policy-makers, there is disagreement over how closely intelligence should support preconceived policy. Some experts and intelligence professionals believe that intelligence should be tailored to the concerns of policy-makers and provide intelligence that is useful and that can be acted upon. This group argues that intelligence that is perceived to be irrelevant to the concerns of policy-makers will be ignored. To be effective therefore, intelligence must be aware of and respond to the policy-maker's priorities and concerns (Hastedt, 1991a, p. 10). Most policy-makers naturally would also prefer receiving intelligence that supports and confirms existing policies. However this runs the risk of corrupting intelligence, of producing 'intelligence to please'. This is particularly a problem with intelligence agencies located within a traditional ministry, such as defence or the foreign ministry. Such intelligence agencies are typically pressured to take into account their parent organisation's policy preferences and budgetary interests, and therefore their intelligence products stand a good chance of being distorted by departmental bias (Shulsky, 2002, pp. 137–138). One of the most frequently alleged providers of intelligence to please was the Defense Intelligence Agency of the US DoD, which was said by its critics to have regularly provided inflated figures of the conventional threat posed by the Soviet Union during the Cold War.

The danger of providing intelligence that confirms policy-makers' preferred options is that it may lead to ignoring danger signals that the policy is misguided, out of touch with developments, or will not have the intended effect. According to those who support a more independent position for intelligence *vis-à-vis* policy-makers, intelligence is supposed to be policy-neutral, providing policy-makers with information and analysis that they need to know, not what they would prefer to hear. According to this view, it is important to ensure the intelligence agency is not part of the policy-making process and that the intelligence process is independent. That is, it is important to maintain objectivity of intelligence and avoid its

politicisation – the exercise of political pressure on intelligence analysts to make their products conform to pre-conceived policy preferences. One of the major challenges in creating effective intelligence structures is shielding intelligence reporting from policy bias and prevailing political concerns, and maintaining sufficient independence to flag new and emerging threats that fall outside the view of established institutional and policy perspectives.

Good governance of the intelligence sector in a democratic state relies on a combination of factors: the need for effective executive direction of the intelligence and security services under its control, but simultaneously a self-conscious exercise of restraint by the executive to avoid overt politicisation of the intelligence product and to allow sufficient independence to see beyond obvious existing threats and the immediate political concerns of the current government (Wilson, 2005, p. 101). It also relies on high professional standards within the intelligence community and the awareness of its members that they operate within the framework of national (rather than governmental) interests, the rule of law, and democratic values. It is the attitudes of those responsible for intelligence, in particular their respect for the law, that will ultimately determine the effectiveness of a system of accountability. Democratic norms and principles must be embedded in the corporate/professional culture of the service.

## Democratic Control, Accountability and Oversight: Definitions

This volume is focused on issues surrounding the democratic control, oversight, and review of intelligence and security services. Although some observers use these terms more or less interchangeably, a case can be made for greater precision in their use. 'Oversight' means supervision, watchful care, management or control.[1] 'Review', in contradistinction, means to view again, survey again, or take a retrospective view of events and activities that have already occurred. Accordingly, a review process, strictly speaking, refers to an *ex post facto* process, whereas oversight suggests more of a watchdog function over ongoing activities of an agency.

Control has at least two key variants. Political control, also known as executive control, is usually used to refer to the direction provided by a Minister through the issuance of guidelines and through monitoring the activities of an agency. Administrative control refers to the internal supervision and management of the intelligence agency as a bureaucratic institution. It also refers to internal rules and regulations. One author has used it to refer to 'the degree to which the Directors of the security and intelligence agencies actually exercise due control over their agencies to ensure that officers comply with the law and proper practice' (Weller, 2000, p. 181).

1. Oversight also has an alternative and opposite meaning in English, which means a failure to notice or consider as in 'Our failure to notice the discrepancy in budget figures was an oversight'.

'Political accountability' refers to the control of the exercise of state power, specifically the behaviour of public officials and involves the possibility of redressing abuses. The notion of political accountability rests on two key pillars: First, the obligation of public officials and agencies to *provide information* about their actions and decisions or to *explain and justify* them before the public and the oversight agencies responsible for monitoring their behaviour. Overlap exists between this dimension and other closely related concepts, such as monitoring and oversight. And second, political accountability rests on *enforcement*, the capacity of an oversight body to *impose sanctions* (punishment) when it has identified improper behaviour by the body being held accountable. Sanctions could involve, for example, an official's removal from office, but softer forms of sanctions also exist, such as public exposure of the wrongdoing. In instances where there were breaches of law, legal sanctions must be applied if there is to be accountability and rule of law upheld. Accountability mechanisms that do not have the capacity to impose negative sanctions are generally considered weaker forms of accountability because they lack the 'teeth' (the power to enforce) that has proven effective in restraining power (Schedler,1999, pp. 14–17).

Oversight of security and intelligence services generally aims to assess one of two things. First, oversight may seek to determine the efficacy of the intelligence service, or its capacity to successfully fulfil its mandate. Efficacy concerns whether a service is making efficient use of public funds and whether it is providing good value-for-money. Executive level oversight tends to concentrate on efficacy issues, such as how effectively the service is fulfilling its tasks and functions, such as identifying important threats, whether the intelligence community is responding adequately to policy-makers' needs, whether it is doing sound analysis, and whether it has adequate capabilities. And second, oversight may seek to identify the propriety of the intelligence service – that is, whether it has acted correctly and complied with legal and ethical norms in its activities and objectives (Whitaker, 1999, p. 131). Judicial oversight is focused on the propriety of intelligence activities, namely whether they have been undertaken in a lawful manner. Legislative oversight tends to mix the two or shift between efficacy and propriety. It may be concerned with the intelligence budget and whether money allocated is an appropriate amount, but also whether intelligence activities are being conducted in accordance with the law (Lowenthal, 2000, p. 133). Public oversight tends to be more focused on propriety issues, often as a function of the lack of available information on efficacy issues. However efficacy also may be addressed, as in the US public debate concerning the failure of the intelligence community to predict or prevent the events of 9/11.

**Framework of Accountability of Security and Intelligence Services**

In order to understand the accountability of public institutions including security and intelligence services, it is useful to consider the tri-partite approach advanced by Schedler (1999). His three-part framework underscores the multiplicity of mechanisms at work concerning public institutions and the various levels at which they operate. Schedler identifies three types of accountability: horizontal, vertical, and the 'third dimension'. 'Horizontal accountability' is the term used to describe the restraint of state institutions by other state institutions, public agencies and the three branches of government (executive, legislative and judiciary). It is considered horizontal because it implies a relationship among co-equals, that is, among independent state agencies.

In contrast, 'vertical accountability' concerns relations among those unequal in their power relations, such as the hierarchical relationship between senior officials (principals) and their subordinates (agents) within a state institution. This can also be referred to as 'control'. Vertical accountability also applies to the efforts of citizens, the media and civil society organisations to keep public officials acting in accordance with good standards (Diamond *et al.*, 1999, p. 3). Citizens, civil society groups and other non-state actors are considered part of vertical accountability mechanisms because they have much less power relative to state actors to influence the target institutions because of the state's control over the means of coercion, resources and means of communication. The vertical accountability process may be top–down, as in the case of principals controlling (having the capacity to determine the actions of) agents in a bureaucracy, or bottom–up, as in the case of citizens holding their elected representatives accountable at election time (Schedler, 1999, p. 23).

The third type of accountability relationship is the 'third dimension'. This refers to the role of international actors, such as foreign governments, intergovernmental organisations and international non-governmental organisations in holding a state institutional actor to account. It could be argued that the European Court of Human Rights, for example, increasingly constitutes a 'third dimension' accountability mechanism for security and intelligence services of EU member states.

*Vertical Accountability*

Applying this framework to intelligence and security intelligence agencies, and starting with the vertical dimension, the executive consists of the highest political level of authority in the state, including the Prime Minister and/or President, cabinet Ministers, appointed advisers and the most senior levels of the bureaucracy. The executive branch is responsible for tasking and directing intelligence services. The mechanisms of control include ministerial directives and policy guidelines, such as those contained within a national security concept. In some systems, the Minister is required to provide direction in writing to the services. The Minister is most directly responsible for exercising oversight but should, in a democratic system, take care not to become too closely involved in the

day-to-day management of the agency, which would weaken oversight and their role as an external control mechanism (Born and Leigh, 2005, p. 55). The Minister requires access to relevant information held by the agency as a function of the executive's responsibility for managing information and policy on national security and for ensuring the proper functioning of public bodies within the security sector, including the domestic intelligence agency itself.

Ministerial abuse of intelligence is a potential problem, as in the politicisation of intelligence, which may result from too close a relationship between the agency and the government. Politicisation of intelligence may appear in the form of intelligence that is tailored to support government policy. There is also the risk that intelligence agencies may be used to gather information on a government's political opponents. Excessive secrecy and the withholding of potentially embarrassing information by the government on the grounds of national security are other potential problems that may flow from executive decisions. These potential dangers require legal safeguards against ministerial abuse and the politicisation of intelligence agencies, such as by establishing the political independence of internal intelligence agencies, granting heads of intelligence agencies security of tenure, establishing legal limits of what agencies can be asked to do by the Minister, and creating mechanisms by which personnel in intelligence agencies can draw attention to alleged abuses (Born and Leigh, 2005, p. 68).

The intelligence and security intelligence agencies themselves exercise vertical control over their members by the Director and senior management of the intelligence service through the issuance of directives, internal regulations and administrative policies. Oversight and review of misconduct may be performed by an internal affairs department. Additionally, a duty to report illegal action and an established channel for doing so is an important development in accountability mechanisms within intelligence agencies (Born and Leigh, 2005, p. 46). Another internal accountability mechanism is the 'whistle-blower', or a public servant who discloses information, presumably to serve the higher public interest, despite his or her obligation for confidentiality and for obeying his or her superior. The whistle-blower seeks to draw public and political attention to an occurrence of corruption, deception or major mismanagement. Accountability is especially served when whistleblowers are guaranteed protection from legal or disciplinary action, enabling them to draw attention of oversight bodies to misconduct.

Traditionally one of the strongest mechanisms for accountability in secret services has been self-accountability through commitment to professional standards and ethics (Franks, 1989, p. 20). Related mechanisms of control and accountability thus include the training and education of employees and a professional code of ethics, peer pressure amongst the agents, socialisation, personnel recruiting, training in legal norms and democratic practices, and the quality and integrity of senior management. This aspect focuses on the norms and values of intelligence professionals in their day-to-day functioning, as well as the attitudes and beliefs of political actors, the media, and members of the public. Norms concerning the political neutrality of intelligence services would also figure here, as would 'honest adherence to the spirit of proportionality, in which the

legitimate level of intrusiveness of security activity, depends on the level of threat' (Wilson, 2005, p. 102).

Obstacles to the agency's control of members derive from a lack of safeguards to ensure legality and propriety, including a detailed legal framework and rules to guide the work of agency personnel. The failure of internal affairs investigations to impose disciplinary sanctions against those who have committed wrongdoing creates an atmosphere of impunity. Members of the executive may also seek to shape the intelligence product or use it to advance their personal, party or special interests, raising the possibility of corruption, abuse of authority or politicisation. The norm of a professional security intelligence agency in a democracy is to maintain a politically neutral stance and to avoid bending intelligence to political needs. Additionally, internal control may be subverted through leaks and whistle-blowers, which, while diminishing internal control especially on matters that the agency does not wish to make known, on the other hand can call external attention to misconduct and spur demands for explanation or punishment, hence potentially supporting accountability.

The other type of vertical accountability is linked to citizens, civil society and the media who perform oversight of security intelligence agencies. Citizen action and mechanisms for holding intelligence agencies and their political masters to account include lobbying, advocacy and educational efforts by individuals, non-governmental organisations and political parties. Those actors normally have access only to a very limited amount of information concerning the activities of security and intelligence agencies. Such information may be voluntarily released, released systematically through legislated declassification schemes, or which may be leaked by insiders or revealed through investigative journalism. Individual citizens and members of civil society groups may use that information to advocate and attempt to effect changes in a state's policies. Academics and other experts who specialise in internal or national security affairs can provide informed analysis of government policies and institutional activities undertaken to protect security, thereby participating in policy debate.

The media constitute an inter-connective tissue linking individuals and groups with government, and play a critical role in conveying information about shifts in public opinion and policy preferences. The media can also play a vital role as a watchdog of government in democratic states. It is primarily through a free press that publics can be informed and government held to account via the threat of public scrutiny of its decisions, actions, and abuses of its power. One of the requirements of a free press, however, is that it operates independently of political control. Furthermore, in order for the media to function effectively as an informal check on power, its members must be willing to question official versions of events, critique policy and decisions of the government, and be imbued with the spirit of investigative inquiry (Pue, 2000, pp. 20–21). Access to information and an independent media are thus vital requirements for keeping government, especially executive government, and its agencies accountable. It not only enables journalists to keep the public informed on state security, but articulates public opinion, voices public concerns, and provides public feedback to security organs.

Inadequate media coverage of security and intelligence issues is often due to a lack of reliable information, which may be a result of strict legal and other constraints on public access to information on national security matters. Further, publishers and broadcasters may face stiff legal sanctions for disseminating such information. Especially when there is no parliamentary committee specifically established to scrutinise the activities of intelligence and security agencies, the role of the media as a conduit for information and enhanced understanding of national security issues by the wider society becomes crucial.

*Horizontal Accountability*

Horizontal control is exercised by entities which are more or less equal in power to the body which is being overseen. A legislature exercises simple oversight when it reviews reports of intelligence services that are submitted to parliament through the relevant Minister, and when it debates issues relevant to intelligence services. A legislature can enjoy a right of scrutiny which might entail the ability to request specific documents and call officials to appear before them and account for their actions. The legislature in a democracy has a role in overseeing and scrutinising intelligence services, often through a specialised committee. Legislative committees usually have clearly defined powers, such as the right to pose questions, issue resolutions, launch inquiries and conduct study missions. A well-developed system of parliamentary oversight provides parliamentary committees with adequate resources (financial, informational and in terms of personnel) in order to effectively investigate the matters under their purview. Additionally, a legislature can vote on the planned activities of intelligence services in a general sense, through the vote on the budget and through a vote of confidence concerning the competent Minister or the government as a whole (Assembly of the Western European Union, 2002b, p. 5).

Problems can arise with parliamentary scrutiny, however. Members of specialised parliamentary committees overseeing security intelligence agencies often have a greater degree of access to information, including secret information, than other parliamentarians. Nevertheless in many democratic systems, even members of legislative committees overseeing intelligence services are usually denied information about operational matters and methods (names of informants, details of operations), which could compromise ongoing operations. Leaks of sensitive information provided to parliamentarians on special committees may damage security and may create distrust among the intelligence services towards the legislators and thwart the flow of information in the future.

As discussed above, intelligence services may also be drawn into party political rivalries and disputes. In parliamentary democracies, it is considered desirable in terms of oversight for the parliamentary committee or subcommittee dealing with intelligence oversight to strive for a bipartisan or depoliticised approach to its functions. That is, the committee members should not seek to use the committee and its oversight powers in intelligence matters to advance their

individual or party interests, but to contribute to the system of checks and balances that help maintain a system of the accountable government.

A practical obstacle to effective legislative oversight and accountability derives from the often superficial nature of the power of the purse. It has been found, for example, that the expenditures for intelligence services are often embedded deeply in a government's overall budget, and in practical terms many parliaments have very limited parliamentary scrutiny over the intelligence budget (Assembly of the Western European Union, 2002a, p. 20). In a similar vein, parliamentary committees can be rendered ineffective through insufficient knowledge of the work performed by the agency and of the issues and questions that need to be addressed. Lack of expertise often is the result when committee members do not acquire long experience on committees.

Another phenomenon that prevents a legislature from functioning effectively as a mechanism of oversight for intelligence and security intelligence agencies is political deference, typically (although not exclusively) found in parliamentary systems with a fused executive and legislative branch. In contrast to a presidential system of government in which there is a separation of powers between executive and legislative branches and a system of checks and balances, in the parliamentary system the executive (cabinet) is drawn from the legislature and power is unified or fused. Since the executive is accountable to the legislature, party discipline is strictly maintained. Political deference may have significant influence on the functioning of parliamentary committees, where members of the majority or coalition governing party are unwilling to criticise a Minister and the domain under his management.

Another obstacle to effective oversight of intelligence agencies by a parliamentary committee is the phenomenon of 'regulatory capture' or 'iron triangles',[2] which may occur when the members of an oversight body identify too closely with the institutional objectives and problems of the agency being reviewed, losing the independent and critical perspective necessary to effective oversight (McCamus, 1989, p. 4). Regulatory capture may result from providing too much secret material to a committee, increasing the chances that the committee members become part of the power structure rather than external critics (Franks, 1989, p. 25).

Another category of horizontal accountability of domestic intelligence agencies is comprised of the courts and judiciary. Their effectiveness as oversight mechanisms can be evaluated in terms of the degree of their independence from the other branches of government. As intelligence and security institutions fall under the executive branch, independence from executive interference or influence is an important determinant of the effectiveness of judicial control. In a democratic state, government powers are subject to oversight by the legislature and review by the courts. Such horizontal mechanisms of control help to ensure that government

2. Iron triangles are recurring interactions among a small set of actors who dominate policy in a specific policy domain. Members of the iron triangle are from executive agencies, the legislature, its committees and staffs, and special interest and lobby groups (McCamus, 1989, p. 4).

actions, which may be motivated by national security reasons, do not violate the rights of citizens and that the government is held accountable for such actions when they do violate rights. Therefore, intrusive measures such as searches and surveillance of persons or premises, wiretaps, orders to obtain confidential records, and spying on political or religious activity should be subject to limits. In such sensitive areas, it is not up to the discretion of the executive branch alone which decides when searches and surveillance are to be undertaken. The courts play an important role in determining that such action is justified, and in imposing limits on executive power to prevent abuses. An intelligence service in democratic state must normally seek a judicial warrant when it wants to perform surveillance and other investigative procedures against a person. The warrant usually is fairly specific in the details of what type of surveillance is to be allowed, against whom, and for how long, and other terms and conditions.

The courts and judiciaries have a direct impact on the protection of rights of individuals and on the exercise of democratic control over state institutions, in particular executive branch institutions. As intelligence and security are realms dominated by executive action, creating accountable intelligence and internal security structures relies especially on judicial review of the legality of government actions, the degree of judicial activism as revealed by willingness of the courts to strike down laws and actions deemed to be unlawful or unconstitutional. In such ways, the judiciary helps to hold government bodies responsible for the use and possible misuse of power. Creating effective, independent and impartial judiciaries is a crucial factor in the development and enforcement of rule of law and therefore of democratisation.

More specifically, the judicial branch is also an important component of creating a security intelligence apparatus that is effective yet limited in its powers, that operates within the rule of law, is accountable, and is subject to democratic and civilian control. In a democracy, the judiciary plays an important role in upholding the law, enforcing the constitution and democratic rights and procedures, and adjudicating disputes that cannot or should not be decided by the executive or legislative branches or private individuals. The judiciary also plays a monitoring role in ensuring that the other branches of government act within the law. Through judicial or constitutional review, the judiciary can prevent the arbitrary exercise of power by the government. Judicial review gives judges the power to interpret the laws adopted by other branches of government, as well as the power to veto those acts. *A priori* or abstract review enables parties to challenge the constitutionality of statutes and decrees before they are enacted. Such review gives a constitutional court real power to influence policy and policy agendas. In contrast, incidental review limits review of government actions to the point after they have been implemented (Ishiyama and Ishiyama Smithey, 2000, p. 167). The review function again underlines the necessity of the judiciary to be independent, as its role in providing effective monitoring of the executive and legislative branches is impossible without freedom from influence by the other branches (Open Society Institute, 2001, p. 19). In the case of internal security,

independent judicial review is essential for the resolution of conflicts between national security claims and the principles of human rights and civil liberties.[3]

The courts and judiciary can be limited as an oversight and control mechanism *vis-à-vis* the intelligence and security intelligence agencies, however, through judicial deference. Even in democracies with the most activist of judiciaries, the courts have traditionally shown deference to the executive branch on issues concerning national security.[4] Equally harmful, however, is the absence of an autonomous judiciary. Judges who are subject to political influence and pressures may be unable to function effectively in their oversight function.

A final category of horizontal accountability *vis-à-vis* the intelligence services is that of independent oversight bodies. The office of ombudsman may be granted the power to investigate and report on a complaint made by the public against an agency. The ombudsman is an independent official who investigates on behalf of the complainant, usually focusing on procedural and administrative failings rather than legal matters, and who usually ends with a recommendation to resolve the problem rather than a binding remedy (Born and Leigh, 2005, p. 105). Another type of independent oversight body is the national audit office, which is independent of the three branches of government in many countries but reports to parliament. An effective audit office is responsible not only for financial audits – auditing the accounts of all public agencies to ensure that expenditures were in compliance with law, but also performance audits of specific project, to determine that funds were spent in an effective and efficient manner (Born and Leigh, 2005, pp. 113–118).

*'The Third Dimension'*

To vertical and horizontal accountability, we can add the third dimension of accountability mechanisms, comprised of international actors, whether foreign governments who provide aid and assistance, intergovernmental organisations that maintain criteria for aspiring members, or non-governmental organisations which seek to influence state actors on specific issues such as human rights and democracy. The biggest obstacle to the effectiveness of the third dimension actors on state security and intelligence agencies is the sovereignty of the nation–state, which in most circumstances enables them to ignore pressures or censure from abroad if it so chooses. Nevertheless, leverage can be exercised when external actors control access to resources or status, as in the case of the leverage of NATO and the EU over states seeking membership in those institutions, such as the majority of formerly communist states in Central and Eastern Europe. Within

3. Principle 4, para. 4, 'Security Services in a Constitutional Democracy'. Helsinki Foundation for Human Rights, Warsaw and the Center for National Security Studies, Washington. 'Security Services in Civil Society: Oversight and Accountability', Report of conference held 30 June – 2 July 1995, Warsaw. Available at http://www.hfhrpol.waw.pl/Secserv/conf_rept/index.html.
4. See the opinion in CNSS *et al. vs* DOJ, United States Court of Appeals, District of Columbia Circuit, 17 June 2003. Available at http://cnss.gwu.edu/~cnss/.

Europe, the European Court of Human Rights (and the European Convention on Human Rights) has exerted growing influence on intelligence accountability.[5]

The preceding discussion of the various accountability mechanisms related to security and intelligence agencies underlines the multiplicity of actors and mechanisms involved in control, oversight, and accountability. It suggests that one should avoid focusing narrowly on legislation and other formal constraints and powers surrounding intelligence services, and pay greater attention to the wider environment of actual and potential accountability mechanisms. While the legal framework is obviously important due to its role in establishing the official mandate of a security intelligence agency and its relationships with other key institutions, the legislature and judiciary, it is not necessarily the most useful or essential approach to understanding control of internal security structures in democratic states. As argued by Lustgarten, law is a secondary mechanism. Of greater and more fundamental importance are basic political values such as respect for dissenting ideas, human rights and privacy; acceptance and legitimacy of a system of effective public oversight; a concept of national security that is limited to core political values and societal interests; and strict requirements for justifying the holding back of information from parliament and the public and restricting the rights and freedoms of citizens. Rather than legislation, it is the internalisation of these political values and ideas within the political culture, especially among the political elite, that provides the most essential indicator of democratic governance of the (internal) security sphere (Lustgarten, 2003, p. 326).

## Structural Problems in Intelligence Control and Oversight

Control of intelligence services confronts at least four main structural problems. The first is the requirement for secrecy. Secrecy makes the management and control of a large governmental bureaucracy such as that of an intelligence service all the more challenging. Secrecy may facilitate the cover-up of unauthorised actions and it makes control by non-intelligence actors more difficult. While an intelligence service is a top–down hierarchical structure like other bureaucracies (each individual being responsible up the chain of command to the head of government), it differs from other government sectors of activity in its fewer and weaker countervailing control mechanisms and processes, formal and informal. These might include audits, challenges or complaints by other parts of the bureaucracy, legislative oversight and press coverage. Further,

5. One of the earliest and most significant judgements of the European Court for Human Rights concerned the Leander case of 1987, following from which all European security services must have their powers governed by legislation, their actions subject to some form of oversight, and citizens with complaints must be able to seek some form of redress. ‘Swedish security police accused of political policing: the Leander case’, *Fortress Europe Circular Letter (FECL)* 52, December 1997. Available at: http:77www.fecl.org/circular/5207.htm.

intelligence's requirement for secrecy and keeping information about activities as tightly guarded as possible prevents spreading it unnecessarily. The institutional culture is one of secrecy and not releasing information except on a need-to-know basis. While secrecy is considered indispensable in intelligence, it also contains in it the potential for abuse, lending weight to what has become one of the most widely used images of intelligence services as a 'rogue elephant',[6] out of control and trampling civil rights and liberties, undermining the relationship of trust that should exist between the intelligence community and policy-makers as well as the general public.

Second, intelligence practitioners are granted a certain (and often significant) amount of discretionary authority in order to fulfil their functions. This constitutes a sphere of autonomy which is considered necessary to avoid politicisation of intelligence and the production of 'intelligence to please'. Professional judgement and ethics are consequently important factors here. However the especially wide scope of discretionary authority enjoyed by many intelligence communities poses a particular challenge to oversight and control, especially when combined with the requirement for secrecy.

Third, policy-makers have tended to find the principle of 'plausible denial' useful in sensitive intelligence operations such as covert action. Plausible denial is the doctrine that 'even if a nation's involvement in covert action becomes known, the chief of state should be able to deny that he authorised or even knew of the action. He should be able to assert, with some plausibility, that it was carried out by subordinates who acted without his knowledge or authority' (Shulsky, 2002, p. 92). Another name for plausible denial might accordingly be 'wilful ignorance'. Plausible denial runs counter to the principle of accountability and insulates top decision-makers and political authorities from the consequences of intelligence operations that may prove controversial if brought to light. Ministers may not want to know the details of any security operations in case these require difficult decisions; security intelligence agencies may prefer to inform Ministers minimally in order to preserve their capacity for plausible denial should an operation fail and prove embarrassing or controversial (Gill, 1991, p. 76).

And fourth, control and oversight of intelligence is made especially challenging by the invoking of reason of national security. A threat to national security can legitimately be claimed to restrict individual rights and justify government actions that would not normally be considered acceptable. Under international law, states can legitimately limit certain basic rights on the grounds of clear and present danger or immediate threat to national security. However various repressive regimes have used these justifications and allegations of domestic terrorism to allow their police and intelligence agencies to torture citizens whom they perceive to be a threat to the regime or government itself.

---

6. This analogy was first used by Senator Frank Church during his chairing of the Senate's 1975 intelligence investigation. He described the CIA as 'a rogue elephant rampaging out of control' for its failed assassination attempt on Fidel Castro and other foreign leaders without clear presidential authorisation.

## Paradoxes in Oversight and Control of Intelligence

### *Dependence of Oversight Committees on the Intelligence Community for Information vs Independence*

In order to be effective, intelligence oversight committee members need to know which questions to ask. This is all the more important since most intelligence professionals would only tell legislators what they asked, and not any more than that. But how does one develop such expertise without becoming captured by the system?

Intelligence is a special area for overseers because of the relative lack of countervailing information and views due to the secrecy of information and programs. Whereas in other policy areas overseers can draw information from sources external to the body being studied, in intelligence there is a high degree of dependence on the subject for information. Mary Sturtevant, a staff member of the US Senate Select Committee on Intelligence, has stated that: 'Because of the classified nature of the programs we review, we are especially reliant on information provided by the very Community we hope to oversee. We lack alternative sources of information and points of view on intelligence budget requests, as there are few constituents with legitimate access to intelligence programs who wish to bring information forward to the Committees' (Sturtevant, 1992).

### *Adversary vs Advocacy Issue*

The relationship between an external reviewing body and the service or agency being reviewed may have an important impact on the flow of information and the quality of the oversight. An antagonistic relationship is likely to raise barriers to information and result in confrontation. However a too accommodating posture on the part of the reviewing body raises the prospect that the overseer has become 'captured' by the agency it is supposed to review and has lost the independence that enables critical oversight. One criticism raised about legislative oversight of intelligence is that intelligence committees may have become co-opted and easily satisfied by explanations provided by the agencies (Center for International Policy, 1996). The problem of co-opting may be made worse in some states by the phenomenon of mobility of former senior staff between intelligence agencies and legislative oversight committees.

In the US a 1996 study by the Permanent Select Committee on Intelligence of the House of Representatives stated that the intelligence oversight committee, in addition to conducting oversight, must be an advocate for the intelligence community, which has no natural advocate in the body politic (US Congress, Permanent Select Committee on Intelligence, 1996). 'Advocacy for overseen agencies is legitimate and to some extent necessary. This has not been an accepted stance for the intelligence committees. We agree with the view of former DCIs (Director(s) of Central Intelligence) that intelligence is such a restricted issue that Congress must be more active in building the necessary political consensus'

(Permanent Select Committee on Intelligence, 1995). This tendency of US Congressional committees to act not as a monitor of intelligence but as an advocate is seen by some as the reason why there was no major reform in US intelligence in the post-Cold War period (Eisendrath, 2000, p. 3).

*Functional vs Institutional Oversight*

Often oversight and accountability are established on specific institutional grounds. That is, legislation mandating oversight refers directly to it occurring with regard to a specific institution, rather than on a functional basis. The problem is that as responsibility for national security becomes increasingly fragmented among many types of government agencies, institutions and departments, the oversight framework may remain tied to a specific institution, while the others escape mandated review or oversight. Reg Whitaker suggests that devolution of the security function has enabled governments to avoid accountability. He has recommended adopting a functional approach, that is, mandating an oversight agency with responsibility for a functional category such as 'security and intelligence', rather than the narrowly defined institutional approach (Whitaker, 1999, pp. 144–145).

*Secrecy and the Public Interest*

Secrecy is vital to the success of many intelligence activities. However overly severe restrictions on information due to security requirements are likely to inhibit public debate and scrutiny of security agencies and activities. Information is vital to enable citizens to be aware of what is going on in their society, to understand what actions have been undertaken by their government in the public interest, and to hold government accountable. As the media fulfils a role as watchdog of government, access to information and measures to declassify confidential information on a regular basis is of vital importance to the process of accountability.

Intelligence agencies and governments tend to over-classify (engage in indiscriminate classification) and to resist efforts to declassify documents after a period of time. Over-classification impedes transparency, oversight and accountability. Ironically, one of the unintended side-effects of over-classification in the US has been said to be the 'erosion of discipline' and growing laxity on the part of officials to observe classification restrictions.

In reaction to withholding of information and official secrecy that is perceived to be excessive, there is also the deliberate action of leaking information to the press and public when there is the belief that doing so is in the public interest. The leaking of classified information by members of the bureaucracy, legislature (Congress) and executive itself has become a major issue in the administration of George W. Bush. While the practice of leaking has been condemned by Bush, many believe that leaks are a necessary corrective when there is too much secrecy and the public interest is not being served by a high degree of

secrecy. However it must be acknowledged that leaks occur for other reasons as well, such as efforts to embarrass political or bureaucratic rivals.

## Challenges for Transitional Societies

Intelligence services inherited from former authoritarian or totalitarian regimes may pose significant threats to the development of new democracies. Intelligence services in repressive regimes are often a key means of maintaining power, and are used to identify domestic political opponents and neutralise opposition to the government. When supporting a repressive regime through 'political policing', these services are frequently involved in human rights abuses, pervasive surveillance and harassment of citizens, extra-legal detention, torture, and extra-legal executions.

How should new democracies deal with those who had committed human rights abuses under the prior regime, while still enabling the service to fulfil its function of providing security intelligence? This may require dismantling the intelligence agency in question, yet at the same time the new regime will need to protect its legitimate security interests. That is, the new regime's intelligence service will require expertise and experienced intelligence professionals, and by necessity will have to draw on personnel from the former security and intelligence services. The task will be to identify and exclude those individuals who were involved in serious abuses, and attempting to ensure that the mentality of those working in the new service does not reflect that of the former service. This would require the process of vetting all employees of intelligence agencies, with particular attention to identifying and excluding those responsible for past human rights abuses. Further, there will likely be specific categories of personnel from the former services who are more acceptable and legitimate as members of the new service because of the nature of their functions under the previous regime. These might include technical experts, for example, whereas those directly involved in political policing would be excluded from employment in the new service.

Also, how much continuity or difference is there in the corporate culture of the democratic regime's intelligence agency from its authoritarian predecessor? Attitudes of impunity may carry over, making the case for even more rigorous oversight and control of these services. Transitional societies must also identify ways to entrench new, democratic and responsible ways of thinking among the personnel of security and intelligence structures. Reform, if it is to be successful, must be embraced and advanced by those within the organisation itself, specifically by Directors and managers (Joffe, 2000, p. 340).

A problem that may be encountered in some post-authoritarian states is certain individuals' use of information and dossiers collected under the former regime's security services to release or sell this material to enrichen themselves or to manipulate the political process. How can the authorities in the newly democratic state prevent those former members of repressive intelligence services from becoming information entrepreneurs and selling their skills, knowledge, records and files or blackmailing key figures in the successor regime?

Another of the issues facing successor states and those in transition to democracy is how to achieve justice and accountability for the abuses committed by the security and intelligence services of repressive former regimes. Public access to the archives of former intelligence agencies is an important effort to achieving justice and accountability. The public dissemination of past activities of state security agencies is a measure aimed at societal reconciliation, especially where pervasive networks of informants were used by authorities for surveillance and control of civilian populations. Transitional societies must also decide whether and how to deal with people responsible for crimes in the context of state security, such as through truth and reconciliation commissions.

The media in transition states encounter special challenges when scrutinising government and state agents. For example, certain observers maintain that journalists in post-communist states remain influenced by traditions of deference towards authority and lack of critical scepticism, especially regarding government policy in sensitive areas such as defence, internal security, and political corruption. Reluctance to pursue certain highly sensitive issues and scandals may stem from a sense of 'civic duty' and patriotism, eroding their professional ethic of informing the public (Mahr and Nagle, 1999, p. 79). Journalists and media outlets may also face legal obstacles in reporting critically on the government and its management of specific policy issues, such as restrictive laws on access to information that has been classified as sensitive, laws prohibiting 'insult' of political figures and public officials, financial and regulatory pressure, and other measures meant to control critical reporting.

On the other hand, it has been noted that in some transition states 'when … there is a generalized feeling that the government repeatedly engages in corrupt practices, the media tend to become surrogate courts. They expose alleged wrongdoings, name those supposedly responsible for them, and give whatever details they deem relevant' (O'Donnell, 1999, p. 30). While the actions of a hyper-vigilant press may force accountability on some wrong-doers, they may also wrongly accuse those who are innocent but who have been deprived of due process in being judged the court of public opinion.

## Conclusion

The challenges of effective control and oversight of intelligence are significant and daunting, particularly in environments where perceived threats to external or internal security are heightened. The paradox of striving for some measure of transparency in an inherently secretive body where information is guarded and often released only on a need-to-know basis is central, as is the degree of professional discretion that intelligence allegedly requires in order to be effective. Nevertheless, the values and norms which are fundamental to democratic systems require that intelligence agencies are accountable and subject to internal control and external oversight. The degrees to which these are achievable in practice remain moot, and subject to considerable variety in interpretation and

implementation, but the principles must be upheld and enshrined as core values in any society that considers itself a liberal democracy.

Developments in the intelligence policy and practice of numerous democratic states since the terrorist attacks of 9/11 have underscored the necessity of retaining their commitment to foundational democratic norms and core values whilst seeking to protect their societies from those who would destroy those norms and values. The attacks of 9/11 instigated an immediate drive among Western governments to implement measures to protect the public safety and national security of their states. In the continuing aftermath of 9/11 in which the Global War on Terror (GWOT) or the 'Long War' is being waged against the perceived threat of international jihadist terrorism, there are significant grounds for doubting whether legal safeguards and oversight and review mechanisms have kept pace with the developing methods and capacities of the intelligence community. Further, there has been little debate on some of the assumptions and assertions used to justify the Long War and the build-up of many states' intelligence capacities, and which have curtailed civil liberties and fundamental freedoms. The ascendance of international terrorism to the top of the international security agenda has created a new and strengthened legitimacy for intelligence agencies, but their missions and targets must continue to be the subject of political and public scrutiny and debate.

The post 9/11 world has witnessed a significant increase in information and intelligence sharing between law enforcement and intelligence agencies, and between intelligence agencies of different countries. It has been claimed that restrictions on information sharing prevented the dissemination of relevant information that could have helped prevent and counteract the terrorist activities of 9/11. There is accordingly now a greater push to better coordinate information sharing internally between government agencies and departments concerned with security, and externally with friends and allies.[7] While acknowledging the necessity to improve effectiveness of coordination among state agencies responsible for national security, intelligence sharing raises important challenges to oversight, review, and accountability, particularly if intelligence-sharing is taking place informally between agencies or more particularly between individuals. Norms of data protection and privacy may be further jeopardised by intelligence sharing between national authorities. To date, these issues have not been adequately debated by the leaders and publics of democratic states.

Democratic oversight and accountability of intelligence services requires constant vigilance from numerous actors, at state level, among the citizenry, and in some circumstances by institutions beyond the state. The framework outlined above, of vertical, horizontal, and third/external dimensions of accountability reminds us of these interconnecting mechanisms of accountability and public oversight, which when taken together may help to mitigate their individual weaknesses. State institutions such as the legislature and judiciary perform an essential role in overseeing intelligence agencies, but may be constrained in exercising oversight by prevailing political conditions, a lack of independence or

7. See for example the fact sheet 'Attorney General's Guidelines for Information Sharing', Department of Justice, 23 September 2002. Available at: www.usdoj.gov.

members' deference to executive authority, as has been in evidence in the climate of fear existing in many states following the events of 9/11 and in the context of a presumed 'Long War'. Civil society and the media perform informal oversight functions which carry legitimacy and may ultimately sway policy but which often lack the institutional means to exert immediate effect. In the context of the current counter-terrorism efforts, the protection of the individual rights and freedoms of citizens of democratic states from possible abusive interference by intelligence agencies and other state institutions is a matter of pressing concern. It is hoped that this volume will contribute to our understanding of the mechanisms of intelligence oversight and control across a variety of national settings, and shine some light on a long occluded area with profound implications for the quality of democratic governance.

Chapter 2

# The Need for Efficient and Legitimate Intelligence

*Fred Schreier*

## Introduction[1]

Intelligence has become an inescapable necessity for any modern government. Only a few states around the world believe that they can do without intelligence services and no state is unaffected by the unwarranted curiosity of its neighbours, nor is any state entirely safe from non-state threats such as terrorism. In a democratic state, intelligence services need not only to be efficient in dealing with these threats, they also need to respond in a legitimate manner. This chapter focuses on the elements of intelligence services which contribute both to their legitimacy and efficiency. For this purpose, the chapter will elaborate on the legal framework of intelligence services; their role in society; their organisation; the relationship between the intelligence producer and consumer; the need for maintenance of secrecy *vs* the need for transparency, and, last but not least; a system of multiple layers of accountability including executive and parliamentary control, judicial supervision as well as informal supervision by civil society organisations and the media.

## Why is there a Need for Efficiency and Legitimacy?

With the end of the Cold War, many believed that intelligence services had lost their enemies and focus, and were searching for new missions to justify their existence. Many voices in Western parliaments advocated a massive slashing of intelligence budgets. Some even proposed the abolition of intelligence services and merging of their functions into other government agencies. Developments proved them wrong. Intelligence again has its place, particularly after 9/11. Even lesser states need it or will soon have more of it. There is plenty to do for intelligence.

---

1. This chapter draws on *Intelligence Practice and Democratic Oversight: A Practitioners' View*, written by the DCAF Intelligence Working Group, 2003.

Today, however, many of the same voices blame intelligence, firstly, for being far too slow, if not incapable, to restructure, reorient, and adapt their activities to the new risks, dangers, threats, and opportunities in the current security environment; secondly, for being inefficient. There is some truth on both accounts. Intelligence services can and should operate more efficiently. In order to do so, the quality, relevance, timeliness and therefore utility of intelligence to the policy-maker must be improved. In some cases, organisational structures create inefficiencies. Some services find themselves with a workforce that is not aligned with current needs yet they lack the ability to correct the situation. Moreover, the growing costs for additional personnel preclude needed investments in new technologies. More administration creates additional inefficiencies. The process of allocating resources to intelligence is often flawed. Moreover, most intelligence services require greater use of modern management practices. Hence, there is a need for more efficiency.

Compared with other institutions of government, intelligence services pose unique difficulties for control and accountability given that they cannot disclose their activities to the public without disclosing them to their targets at the same time. As a result, intelligence services are neither subject to the same rigours of public and parliamentary debate nor to the same scrutiny by the media as other institutions of the government. Their budgets are secret; their activities are secret; and their products and achievements are secret.

For the public, the perceived lack of accountability is troubling. Intelligence is not only seen as mysterious, but often as uncontrolled, working outside the law, and not obeying the national policies. Moreover, a few intelligence services have experienced highly publicised espionage cases, which have caused damage to national security and which have raised concern not only about the failure of intelligence to detect spies in their midst, but also about the degree to which these services hold accountable those responsible.[2] Hence, there is a need for more legitimacy.

Legality, and thus a legal framework for intelligence, is the base and starting point. Intelligence as a separate yet inseparable part of democratic forms of government is not only accountable to the executive, but also to the representatives of the people, and ultimately to the people themselves, who − as taxpayers − finance them. In order to attain legitimacy, effective control, and accountability, oversight mechanisms are needed. Only then will the public and their representatives begin to trust and respect intelligence services. And only then will intelligence services become an accepted part of the nation-state.

While the basis for legality is a legal framework for intelligence services, legitimacy can, however, only be achieved if democratic control of intelligence services is perceived to work and the value of accurate knowledge and unbiased intelligence is recognised as a condition of good governance in the globalised world. Since in some countries democratic control of intelligence services is not

2. A notable example of such a case is that of 'Rainbow Warrior', which is further discussed in Chapter 8, 'Checks and Imbalances? Intelligence Governance in Contemporary France', in this volume.

yet fully established or working, both the essentials of a legal framework and for the democratic control of intelligence services will be presented.

## A Legal Framework for Intelligence Services

Intelligence requires the enactment of a legal framework which must define the area of responsibility and authority of the services, the limits of their competence, the mechanisms of democratic control, as well as the legal means to deal with complaints in cases of violation of rights (Born and Leigh, 2005). A system of statutory regulation, coordination and control is needed to guide intelligence work. This system could be subdivided into laws, executive orders, directives, and ministerial or agency regulations.

The basic missions, responsibilities, restrictions, structures, and relations among the intelligence services associated in an intelligence community should be established by national law. The law has to set limitations which, in addition to data protection and other applicable laws, achieve the proper balance between the protection of individual rights and the acquisition of essential information. Ideally, the law should not be construed as authorising any illegal activity nor should it provide any exemptions from any other law. Ministers responsible for intelligence services must have responsibilities under the law. In addition, each service has to have a statutorily defined relationship with its Minister and a legally defined position in relation to that Minister.

Ordinances or executive orders should define functions and organisational matters; list duties and responsibilities; establish procedures and measures for coordination, assistance and cooperation; impose restrictions etc. Implementation of executive orders and subjects prone to rapid changes, such as collection and analysis requirements, objectives and priorities, plans, programmes, and resource allocation, etc., require more detailed directives which can be established in two varieties – unclassified and classified.

## The Role and Functioning of Intelligence Services

Informed decision- and policy-making require adequate intelligence, assessments and warning. Only if Ministers, top executive officials, and their planners and counsellors are sufficiently informed about the state of the world, the likely developments, and the existing and potential threats, dangers, risks, and opportunities, can they be expected to make sound judgments in the areas of internal and external security, national defence, and foreign relations.

Intimate knowledge of the strategic situation, possible and probable developments, the risks, dangers, threats, and opportunities are a prerequisite for (1) the definition of national interests, (2) the development of an adequate security policy and sound national and military strategies, (3) the determination of the missions of the armed forces and the security forces, and (4) the establishment of doctrine and its translation into operations. Moreover, this knowledge, contingency

planning, and timely warning are the prerequisites for efficient and effective national crisis management. Intelligence services provide the basis for this knowledge. Moreover, they also must, at all times, be able to warn of impending crises and to detect possible threats in advance. With smaller military forces, the warning function grows in importance, with very early warning becoming a necessity.

The rapid evolution of the strategic, political, and economic environment since the end of the Cold War has enlarged the quest for information on security issues that governments will have to pursue. With conventional military threats diminishing, new risks and dangers connected with globalisation, destabilisation, terrorism, proliferation, and organised crime have gained importance. Three trends in particular will mark the foreseeable development in Europe that will multiply the security challenges, render assessments more complex, developments less predictable, and crisis and conflicts less calculable (DCAF Intelligence Working Group, 2003, pp. 6–7):

- The multiplication of actors, sources of crises, and means of conflict, which will render threats, crises, and conflicts multidimensional.
- Increasing transfer of foreign violence into the domain of internal security and into urban areas, with more ethnically, religiously, and economically rooted societal strife in new and mainly asymmetric forms of conflict, thus undermining the state's right of self-defence.
- Growing economic interdependence, accelerating technological developments, increased interconnectivity of information and communications, and the multiplication of international relations will enlarge regional and global interdependence and concomitantly national vulnerabilities.

In a world where borders have dissolved and foes increasingly operate not on conventional battlefields but in a grey area where traditional notions of crime, terrorism and armed conflict overlap, national security is becoming ever more dependent on regional and global stability and the solidarity of like-minded nations. Since geographical distance can no longer provide adequate security, states have to influence crises and conflicts abroad and focus security and foreign policy ever more on crisis prevention, crisis reaction and peacekeeping in coalition with the able and willing.

In the wake of the information revolution, it is generally believed that a worsening of the security situation will be preceded by fairly clear signs reported by the media and available for anyone interested in drawing conclusions. However, volume of information does not equal useful information, especially since the media also contain a lot of disinformation, second-guessing and speculation, all under the guise of real information. The question therefore remains as to whether governments would be well advised to rest national security on what the media can find out. The conclusion is obvious. Governments can and should take advantage of information that is openly available. However, since states have an absolute

obligation to their people to make sure that new and serious threats are detected in time to counteract them, there can be no substitute for intelligence services. Though the debate will be continued by those who argue that open source information far outweighs in value the expenditure and effort devoted to intelligence services, there is no such argument inside governments. Governments understand that what is sought clandestinely is that which cannot be obtained openly, including confirmation. Hence, all-sources intelligence is needed to discover what is really happening.[3]

The set of tasks assigned to intelligence services is both more complex and more numerous than during the Cold War. What has dramatically changed for intelligence services is the number and diversity of risks, dangers and threats (Berkowitz and Goodman, 2000, pp. 99–123). Despite the inequality of states – in some of which sovereignty remains a myth, if not a hypocrisy – there are also rogue regimes which promote destabilisation, produce weapons of mass destruction, provide sanctuary for terrorists, and sponsor the assassination of political opponents abroad. There are 'failing' or 'failed' states characterised by endemic conflict, chronic warfare that has become a lucrative economic enterprise, genocide, humanitarian disasters, and mass-migration. And there is also a growing number of powerful non-state entities. While some multinational corporations or charitable non-governmental organisations (NGOs) might be honourable, others, like some financial institutions or monopolistic media organisations are more questionable. Quite another set of non-state actors are international terrorist organisations; ideological, ethnic or religious extremists; and mafias and large criminal organisations, which present a serious and dangerous threat to all societies. Taking advantage of the opening of borders and skilfully using the discrepancies between various national laws and judicial procedures, terrorists, extremists, war criminals, weapons and drug dealers, smugglers, specialists in the laundering and recycling of dirty money, or in the clandestine disposal of noxious waste and polluting materials, often remain unpunished and prosperous. Where law enforcement structures remain ineffective, the balance sheet is clearly on the side of crime and not of the law. Moreover, there are some new intelligence services and – since it is now fashionable to reject the bureaucratic state and to transfer its tasks to the private sector for the sake of efficiency and cost reductions – all sorts of private military, private security and private intelligence organisations which require some monitoring (Berkowitz and Goodman, 2000, pp. 7–12).

These actors, and even more so the terrorists and criminals exploiting the internet, as well as other offenders engaged in hacking and information warfare, have made the problem of predicting what their next moves and targets are going to be many times more complicated. All means of collection have to be exploited in a systematic way to find intelligence and evidence, foremost about intentions, plans and capabilities, but equally about the organisation, communications, resources, and movements, of these widely diverse groups or cells of globally spread networks.

3. For an elaborate discussion on open sources, see Treverton, 2003, pp. 93–135.

The rule for tasking intelligence services has always been to go after that which cannot be acquired more easily, more safely, or more cheaply by any other means. Methods of collection have changed dramatically during the course of the twentieth century – satellite imaging and electronic interception are the most obvious evidence of this and have become the tools of choice. However, an often undervalued aspect is continuity, which for smaller countries is of particular importance. Discontinuing a particular intelligence competence raises the prospect that it cannot be recovered with much hope of success some years later. Politicians and officials with little exposure to the production of intelligence often think that the services can mothball competence and keep it going on the backburner for bad times. In most cases this is not possible. Even less understood is the fact that if intelligence is not alert when a new technology is introduced, it will find it very difficult and often impossible to catch up later. At least in the technical field, the truth is almost always that if intelligence does not remain actively engaged, it risks being left out in the cold for a very long time, even if the government is willing to spend a lot of money to catch up and repair its capabilities. Hence, what is needed in order to succeed is continuity and cooperation with like-minded friends.

New non-military threats and international operations are opening the way for more advanced cooperation between security and intelligence organisations from participating or interested countries. One reason for this is that nobody can effectively cover all of the places throughout the world where such activities may take place. The efficiency and economy of such intelligence work can be greatly enhanced through cooperation and sharing between intelligence organisations.

Bosnia and Kosovo have represented what appears to be the new pattern of intelligence support for international intervention of all kinds. All those responsible for such operations, from the United Nations (UN) Secretary-General downwards, have emphasised the need for good intelligence. National intelligence is relied upon to fill gaps, validate other sources and above all, assess threats. The goals of graduated force, surgical strikes, low casualties, and minimum collateral damage are all intelligence-dependent. Military forces deployed in peace-enforcement and peace-building require virtually the full range of wartime intelligence support. Providing evidence on crimes against humanity now adds a whole new set of intelligence requirements. Kosovo has demonstrated the paradox of highly public international operations depending crucially on secret intelligence.

The UN, European Union (EU), North Atlantic Treaty Organisation (NATO) and other regional institutions will eventually develop machinery for supranational intelligence assessments, but it will be a long haul and will have to build on interstate exchanges. The United States (US) is already committed to intelligence support for international organisations. To some extent, this is already a *de facto* underpinning of international society. Yet, for credibility, the American input needs to be complemented by national intelligence institutions capable of critically assessing it for their own governments.[4]

4. However, states are reluctant to share intelligence, even with allies in post-cold war multilateral peacekeeping operations in order to protect intelligence sources and methods. See Lowenthal, 2003, p. 59.

Intelligence contributions to international security are not limited to specific situations in the context of conflict prevention, peace-keeping, peace-enforcement and peace-making, such as in negotiating a peace settlement, but extend to a group of world-wide and long-term security issues. Wide-ranging, intelligence-driven cooperation is currently being undertaken in the fight against terrorism, where intelligence is the most critical resource in the limitation of weapons of mass destruction and other arms proliferation, the support of the many agreements that now exist for arms control and other confidence-building measures, and for enforcing international sanctions. International arrangements between intelligence services underpin these political agreements, where national intelligence tips off collaborating nations or is used to keep them from backsliding.

## Mission and Organisation of Intelligence Services[5]

Since the purpose of intelligence services is to inform government – that is, telling truth unto power – their first and main task is the collection and evaluation of information, its transformation into intelligence, and dissemination of warnings, risk estimates, situation reports, and assessments according to the needs of the national government.

The second task is counterintelligence: the acquisition of intelligence and evidence on, as well as actions designed to neutralise, hostile intelligence services. Activities might involve espionage against such services, turning agents, debriefing defectors, and analysis of the methods and means of hostile services. They may also involve the penetration of those services and disruption of their activities.

Traditionally, democratic states separate *domestic* from *external* intelligence services. This can be justified by the different missions and by the fact that different rules and laws apply to intelligence operations on national soil and abroad. The mission of *domestic intelligence* generally is to obtain, correlate and evaluate intelligence relevant to internal security. Internal security means the protection of the state, territory, and society from acts of espionage, sabotage, subversion, extremism, terrorism, organised crime, narcotics production and trafficking, arms and other smuggling, dissemination of child pornography, etc. The mission of *external intelligence* generally is to obtain, correlate and evaluate intelligence relevant to external security and for warning purposes. Maintenance of external security requires knowledge of the risks, dangers, and threats, as well as of the opportunities and likelihood of external events and outcomes. Hence, information is needed about intentions, capabilities, and activities of foreign powers, organisations, non-state groups and their agents that represent actual or potential threats to the state and its interests.

In some states external intelligence services have the task of covert action: activities or operations – including the use of violence − designed to influence foreign governments, NGOs, and other non-state groups, persons, or events, in

5. For an elaborated discussion on the goals and organisation of intelligence services, see Herman, 1996, pp. 16–35.

support of the government's foreign and defence policy objectives while keeping the sponsoring government's support of the operation a secret.

Information held by domestic intelligence agencies, as well as the techniques by which it is collected, should in principle be subject to national laws, including laws on data protection. Where exceptions to these laws are required for operational reasons, they should be the subject of separate laws or ordinances. All operations should be carried out with the approval of a member of the government, ideally of the Minister responsible for the domestic intelligence agency.

On the other hand, external intelligence services could scarcely do their work if they were to obey every law of the countries in which they operate, especially if those countries are not democracies. However, principles and rules should be established, agreed at the political level of government, about what external intelligence services can and cannot do in a particular country.

Counterintelligence is the national effort to prevent foreign intelligence services and foreign-controlled political movements and groups, which are often supported by intelligence services, from infiltrating the state's institutions and establishing the potential to engage in espionage, subversion, and sabotage. Counterintelligence also deals with acts of terrorism, regardless of whether they are initiated at home or abroad. It involves investigations and surveillance activities to detect and neutralise the foreign intelligence service presence, the collation of information about foreign intelligence services, and the initiation of operations to penetrate, disrupt, deceive and manipulate these services and related organisations to one's own advantage.

Counterintelligence differs from intelligence gathering, in that it exists to counter a threat, whether from hostile intelligence services or from non-state groups, and is thus to some degree reactive. With few exceptions, counterintelligence results are not produced in the short term. And counterintelligence investigations cannot be limited to arbitrary time periods.

There is no need for an independent counterintelligence service which might tend to become another bureaucracy interfering, delaying, disrupting and attempting to usurp the intrinsic counterintelligence functions of each of the services. However, there is a need for a centralised counterintelligence programme, the purpose of which is to integrate, promote, improve and coordinate the counterintelligence operations, investigations and research of each of the services.

Close cooperation between both external and domestic intelligence services is required if the counterintelligence effort is to be effective. For example, a group of extremists carrying out armed attacks might be planning those attacks within the country, and therefore seek to develop operational intelligence to support this policy (domestic intelligence), but may be supported from a neighbouring state where it does its training and planning (external intelligence). A centralised counterintelligence programme establishing authoritative coordination and cooperation between the domestic and external intelligence service on counterintelligence matters, which inevitably cross borders, will preserve the legitimate jurisdictional demarcation between domestic and external counterintelligence responsibilities.

Different intelligence needs often lead to the creation of several services instead of one comprehensive organisation. The ministry of defence will often have an intelligence service of its own, concerned with more technical issues such as the assessment of the military potential of neighbouring states, defence industries, military personalities, etc. In order to determine its own weapons requirements, the defence ministry intelligence must know the nature of potential hostile forces as well as the characteristics of the target base. Size, capabilities, location and readiness of those forces must be continually monitored, either as a guide to planning requirements or as a means of warning against possible attack. Much of this information is also important to negotiation and monitoring of arms limitation agreements. Hence, defence or military intelligence can also be viewed as a third branch in addition to external and domestic intelligence.

Different collection methods, especially with sophisticated technical means, can also give rise to specialised intelligence organisations. These include imagery, signal and cryptologic intelligence agencies.

Since risks, dangers and threats are of expanding transnational reach and impact, ever more information is collected by different services and means on the same subjects. The traditional limits between external, domestic, and also criminal intelligence are becoming increasingly blurred with overlapping missions and objectives, increasing the opportunities for misunderstandings and rivalries. There is notable convergence in countering terrorism, international organised crime, and proliferation. Thus, the separation of domestic and external intelligence services is becoming more artificial, hence questionable. Another type of cooperation seems to be necessary at the European and the international level. While separation might still be a good solution for great powers with large intelligence services, it will require an ever greater effort for coordination and control, better regulated access to each other's information and assurance of production of joint assessments. This is why smaller countries with fewer resources might prefer to have just one intelligence organisation. This avoids wasting efforts, resources, and time; solves the risk of unhealthy competition between different agencies; simplifies contacts, information sharing and cooperation with foreign intelligence services; facilitates high level subordination of intelligence in the state's hierarchy and cooperation and coordination with other ministries and government agencies; and simplifies control and oversight of intelligence. Amongst others, the Spanish *Centro Nacional de Inteligencia* (National Intelligence Centre, CID), the Dutch *Algemene Inlichtingen en Veiligheids Dienst* (General Information and Security Service, AIVD), and the Turkish *Milli İstihbarat Teşkilatı* (National Intelligence Organisation, MİT) are examples of democratically controlled 'fused' intelligence services, which have found solutions to the problem of different rules and laws applying to intelligence operations on national soil and abroad.

It is a good rule however, that intelligence must be separate from law enforcement. Law enforcement and intelligence have fundamentally different purposes. While the goal of law enforcement is to get a conviction in a specific criminal case, the task of intelligence is to collect as much information as possible on potential threats to the state and society. An intelligence service thus might prefer not to arrest an identified criminal if this would reduce its capacity to collect

further information. An intelligence service might also not want to divulge its information in an open judicial process for fear of betraying the source of its information.

But the function of criminal intelligence − the collection of information on organised crime − requires skills which are similar to those used by intelligence agencies. In certain circumstances, targets of domestic intelligence services might be involved in organised crime as well, so the interests of the two organisations would overlap. Yet intelligence agencies usually have no authority to conduct criminal investigations, no power of arrest, and no power to search homes. Hence, when it is clear that a crime has been committed, the collection of evidence and execution of arrests should be carried out by a specialist branch of the police force.

For domestic intelligence, the criteria for legal surveillance and investigation in a free society is the question of violence. Domestic intelligence is justified in targeting an organisation if it, or its influence, has led to violence, or if there is a reasonable apprehension that it will. However, the application of law and the exercise of executive power against violence is for the field of law enforcement alone. Coordination and cooperation between these organisations has to be ensured at ministerial level.

Nonetheless, the requirements of national security and protection of the state may occasionally be at odds with established concepts of privacy, civil liberties and civil rights that the state grants its citizens. Clearly, if domestic intelligence services had no special empowerments, they would find the protection of the state a very difficult task. Conversely, domestic intelligence services with unlimited powers might find the protection of the state easy, but would cause unacceptable damage to the rights, civil liberties and privacy of citizens.[6] In a democratic state, a trade-off between these diverging interests has to be found in a manner that is politically and legally sound. This implies a conscious decision about what is permitted and what is not. The government must therefore lay down general principles for what is acceptable, and ensure that these principles are transparent, known to the public, and adhered to by the intelligence services. Comparable considerations apply, albeit in a different fashion, to external intelligence services.

## The Relationship between the Intelligence Producer and the Consumer

The relationship between those who collect and evaluate intelligence and those who use it in the preparation of state policy – the providers and the consumers – is of great importance (Treverton, 2003, pp. 179–184). Intelligence knowledge is itself of two overlapping kinds: first, the product of special, largely secret

6. For member states of the Council of Europe, the European Convention of Human Rights and case law of the European Court of Human Rights have set standards and limitations for special powers of intelligence services to interfere with private communication and property. See Iain Cameron, in Born, Johnson and Leigh, 2005.

collection and, second, assessments on those subjects, mainly bearing on national security, on which the intelligence community is the national expert. The common factor to both is some separation between intelligence and policy-making. If truth-seeking by the intelligence producers is linked with governments disposed to listen, the result is an improvement in the perception of international actors, events and processes. The Western idea of objective, all-source intelligence assessments on security, defence and foreign affairs, with some separation from policy-making, is a necessary part of the modern, global standard of government. Intelligence can err by striving too hard to be 'useful' to its customers, but this is balanced by the ethics of professional objectivity, the practitioner's self-image of 'exposing all those who won't listen to all the things they don't want to know', and the importance of international reputation. Intelligence provides no magic key to the future. But it can do something in favourable conditions about governmental ignorance and misperception. The effect over time is that governments that take note of intelligence behave more effectively internationally than those that operate without it. However much intelligence is criticised for its failures, democratic rulers are in trouble with their electorates if they are known to have disregarded or even to have ordered the failure.[7]

Intelligence is only as useful as political leaders permit it to be. Personalities play an important role and can stimulate or limit the interest for intelligence. Therefore it is vital to have a central organ within a government that can follow the production of intelligence to evaluate which means of collection gives the best results according to the needs. Ideally, coordination of intelligence collection is handled by an executive branch entity at the highest level – for example the US National Security Council – that advises the President or the Prime Minister with respect to the integration of domestic, foreign, foreign economic and military policies relating to national security. This entity can provide review, guidance, and direction of the conduct of all domestic and external intelligence activities. Since this entity is concerned with national policy, it has a profound interest in making sure that intelligence guides, and does not follow, national policy.

In smaller states with few services, intelligence production can easily be passed directly to the National Security Council. For great powers with many intelligence agencies this is impracticable. Although specialised agencies support the information needs of specific intelligence customers, they make comprehensive national assessments more difficult. In addition, agencies are sometimes tempted to compete with each other, emphasising things which they each believe to be important. Some kind of coordinating mechanism is therefore required to ensure that government is presented in a timely manner with the most complete and objective intelligence picture possible. This could be in the form of an independent national assessment staff or an authoritative executive coordinating organisation that collects and assesses intelligence from the various agencies. Coordinating all-source intelligence in a form that makes it both accessible and usable for policy-

7. Hence the desire of political leaders to resort to plausible deniability, that is to deny that instructions were given or to deny that they were informed. See Born and Leigh, 2005, pp. 65–66.

makers while at the same time giving appropriate weight to dissenting opinions is the intelligence equivalent of squaring the circle. So far, no fully satisfactory method for achieving this miracle has been devised. But production of joint assessments should ideally be undertaken by a staff not necessarily attached to the agencies which produce intelligence.

Unless all relevant information is marshalled when assessing intelligence on a subject, the quality of the finished product might suffer. Hence, covertly obtained intelligence should not be assessed in isolation from overtly obtained intelligence. Secret intelligence is the continuation of open intelligence by other means. So long as governments conceal a part of their activities, other governments, if they wish to base their policy on full and correct information, must seek to penetrate this veil. This may entail varying means and methods, but ultimately secret intelligence must complement the results derived from the rational study of public, or overtly available, sources. This, in essence, is the job of the independent body or national assessment staff which produces joint assessments.

Often, it could even be useful to involve independent experts, such as diplomats or policemen, in the production of the final joint or national assessment, since they will have their own insights and experience to contribute. Outside experts brought into the process, however, must necessarily have the needed background, including intelligence training and experience. Bringing in distinguished outsiders, as well as experts, would not guarantee that differences with state policy would be brought to the fore, but it would facilitate the national assessment process, especially if coupled with more competitive analysis of the intelligence agencies.

**Maintenance of Secrecy**

Transparency of the government, the state administration, and the activities of all agencies is important in a democracy if the government wants to retain acceptance by, and support of, the electorate. However, for intelligence services to fulfil their missions effectively, there are some sensitive domains of activities which have to be, and must remain, secret. In democracies, at least three generally agreed items of intelligence are sensitive:

1. All information pertaining to sources, operations, methods, procedures, and means engaged for collection.
2. The identities and activities of the service's operational staff and protection of its knowledge.
3. Origin and details of information, intelligence and assessments provided in confidence by foreign governments or foreign services.

All intelligence services require maintenance of secrecy on those issues. They must be able to guarantee protection of the identity of sources as well as protection of the information received in confidentiality. This must be not only for themselves

and for the protection of their personnel, but also for the people in the outside world who work with the services. Secrecy is needed because it is the only way to assure potential sources of their own safety. No one will volunteer to work for an intelligence agency unable to prevent public disclosure of its sources.

The need for anonymity of the service's operational staff and their activities follows from the first item: sources, operations, methods, procedures and means cannot remain secret if the personnel engaged in operations are known to the public. Also, all too often intelligence successes must remain secret in order to ensure continued successful intelligence collection.

The knowledge of the intelligence services needs to be protected since disclosure could reveal intentions, the specific targets of the collection effort as well as the capabilities of collection systems – disclosures that could lead to effective countermeasures, disruption of operations, denial of access and collection in the future.

If the government is interested in, and seeks the cooperation of, its intelligence services with the intelligence services of foreign countries, maintenance of secrecy of the origin and the content of information, intelligence, and assessments provided is essential. All documents and carriers of intelligence remain the property of the providing nation and cannot be further disseminated, nor declassified, without the originator's permission. Therefore, a later transfer of these documents to the national archives is not advisable. The mere request to a foreign intelligence organisation for such permission, and for declassification, could easily foster an atmosphere of concern, not only over protecting sources and documents passed previously, but also whether it should continue to do so. Since one's own intelligence information has to be made available to those foreign services under arrangements for intelligence sharing, maintenance of secrecy is equally expected from those foreign services.

Hence, it is necessary to establish clear guidelines, rules and directives for the classification of, distribution of, and access to intelligence with respect to citizens, as well as foreign government agencies. Regarding the documents of the individual intelligence services, these directives also have to cover appropriate archiving of records, procedures for declassification, review of sensitive intelligence products, and standards for declassification.

However, not everything ought to be protected and kept secret. Not all intelligence services can offer data to the public on their official websites like the 'World Fact Book' of the Central Intelligence Agency (CIA), much used and highly appreciated in the academic world. Only big services have the resources to keep such data up to date. But intelligence services could sanitise some of their products and assessments of current interest, and make them available to the public, particularly when such publications can help to factually clarify controversial issues, developments, events, and positions of the government. In addition to a favourable public attitude towards intelligence, which is desirable and needed in democracies, public collaboration is also important. By providing a public telephone, fax and e-mail address, services can encourage significant public support. In this respect, the services of various countries (for example the Netherlands and the United Kingdom) publish a

yearly public report including general information on policy, performance, staff and budget. Clearly, secrecy should not be misused for covering up mismanagement, failure or corruption. For this reason, secrecy should not obstruct a minimal level of transparency, necessary for effective accountability mechanisms to exist between the services and their overseers in the executive, legislative and independent institutions such as the national audit office and inspector-general.

## Democratic Control of Intelligence Services

A state's system of democratic control is the product of its system of government, politics, history, and culture. As there are many different cultures and political systems, many different norms and practices of democratic control exist. As there is no single model for democratic control, neither is there a definitive normative model for democratic control of intelligence services.

In democracies, democratic control of intelligence services and their activities is exercised by executive, legislative and judicial entities, and, indirectly, by the public. Every element plays its specific part in one entire package of democratic control and accountability, the purpose of which is to provide assurance of legality, proportionality and propriety for activities that are necessarily conducted in secret.

Within this package, executive control and accountability plays the decisive role. The higher the echelon of executive control and the more seriously it executes its tasks, the lower is the likelihood of problems accruing to the government from legislative and judicial oversight. It is the executive which is fully responsible for proper auditing and controlling of the intelligence services, thus creating the necessary base for transparency and parliamentary control.

### *Executive Control and Accountability*

Intelligence services as a separate, yet inseparable, part of the government must act according to the policies of the sitting government and in pursuit of objectives relevant to these policies. But the secrecy which surrounds the work of the intelligence services can produce temptations to act independently. Thus, there must be a clear tasking system, controlled not by the intelligence agencies themselves but by the government departments on whose behalf they are collecting information. As a principle, no intelligence operations should be conducted unless there is an agreed requirement. There is an obvious need to provide constant and competent political guidance to the services, to raise their accountability and redirect them to new tasks. However, the misuse of intelligence services by an elected government for its own political ends must be excluded. Hence, intelligence services should not be affiliated with any party and they should be depoliticised.[8]

8. For further discussion on the issue of ministerial abuse of intelligence services, see, for example, Born and Leigh, 2005, pp. 68–76.

Generally, the more ministerial interest in, and attention to, the work of the service exists and develops, the more intimate the service will become with the conduct of the daily business of the government, and the more the service will be subject to checks and balances. But this alone is not sufficient. The services must have assurance of the legality in things they do. Therefore the intelligence community requires laws and regulations that guide their activities, and a system of coordination and a number of statutory mechanisms for the accountability and control of their work.

Intelligence services need a statutory regime that arranges the authorisation of the ways in which they collect intelligence to ensure that issues of necessity and proportionality are properly considered ahead of the event. The most intrusive of these methods should require the signature of the Minister. In some countries that role of authorisation falls to the judiciary, but the executive is bound to be in a better position to determine what should be the policy to adopt on internal and external security and national defence than a tribunal, no matter how eminent. The statutory regime should have a bearing not only on how services collect and administer intelligence, but also on how they have to use it. Services should be accountable for the ways they use intelligence. It should define what information is sensitive, deal with classification levels and authority, downgrading and declassification, safe-guarding classified information and so forth.

One of the main tasks of executive control and accountability is to make sure that the intelligence services are functioning properly, that is, that they ask the right questions, collect the right information and respond to the decision-makers' needs. Of particular importance for executive control is to identify intelligence failures and take action to prevent them in the future.

The source of executive control and accountability should ultimately be either the President or the Prime Minister. There are practical reasons why the President or Prime Minister or the Minister responsible might not be able to give full attention to all of the control tasks. Thus, governments in democracies will normally appoint individuals or establish committees or boards mandated with supervision of intelligence activities. Individuals can be appointed as inspectors, controllers, efficiency advisors, and so on, who report to the President, the Prime Minister or Minister. Committees or boards can be established that ideally report to the National Security Council, alternatively to the President, the Prime Minister or the Minister responsible. These can be constituted by individuals outside of government, qualified on the basis of ability, knowledge, diversity of background, and experience. However, no member should have any personal interest in, or any relationship with, any intelligence service.

Some countries have executive committees for intelligence oversight and for policy review to scrutinise intelligence performance and policy. The mission of an intelligence oversight board can be to:

- review periodically the internal guidelines of each service concerning the legality or propriety of intelligence activities;

- report periodically on its findings and any activities that raise serious questions of legality or propriety;
- forward judicial oversight reports received concerning activities in which a question of legality has been raised;
- conduct such investigations of the intelligence activities of the services as it deems necessary to carry out its functions.

In comparison, the mission of a policy review committee can be to:

- establish requirements and priorities for intelligence;
- review the intelligence programme and budget proposals, and report to the government, the Minister or Prime Minister as to whether the resource allocations for intelligence respond to the intelligence requirements of the government;
- promote collaboration and intelligence sharing between the services, and provide checks and balances within the system;
- conduct periodic reviews of intelligence products, evaluate their quality, develop policy guidance to ensure quality intelligence and to meet changing intelligence requirements;
- submit an annual report;
- make recommendations on intelligence matters.

Auditing is another important part of executive control and oversight. In democracies, an external audit of the accounts is normally done by the national audit agency or office.

*Legislative Oversight*

There are different models for legislative oversight of intelligence activities (Born and Leigh, 2005, pp. 77–104). Arrangements that match the legal and constitutional arrangement of that particular country are needed, not those that look attractive from another country. But any arrangement that removes the ultimate responsibility for accountability of the conduct of government business from ministers in parliament would be a mistake. Few members of parliament have expertise in national security or intelligence matters at the time they are elected. Those in the executive branch, by contrast, have mostly been selected for their positions precisely because of their expertise in some aspect of national security affairs. Hence, to substitute somebody else as the final arbitrator of what should happen is wrong.

Parliament's budget authority gives it control over the intelligence budget. However, intelligence is not just another form of public expenditure. Since it is intelligence, it brings with it certain inherent problems that can restrict and hamper parliamentary involvement. This is why there should be a special parliamentary committee expressly charged with oversight of intelligence, which can appropriate the funds necessary, and which keeps track of how the funds are spent. In some

states, parliament also has control over the appointment of agency heads, and plays a role between the services and the public.[9] The nature of intelligence limits the information that can be provided to the public. As representatives of the public, the parliamentary oversight committee needs access to secret information. It should have the right to request reports, hold hearings, and conduct investigations to expose shortcomings or abuses, but it needs to maintain secrecy. Members who serve on this committee ordinarily come to appreciate the rules governing the disclosure of intelligence and why they are important. In order to be able to perform this task, these parliamentarians must have the trust of both the intelligence services and the public. Moreover, the right of the political opposition to participate in oversight should be defined.

However, the parliament's oversight committee must not have the authority to direct the intelligence services to initiate certain investigations or to pursue certain cases. The question of which persons or groups to investigate is an executive branch decision. Moreover, the committee is a political body, subject to political expediency and to overreaction. The members of the committee should have a responsibility to avoid overreaction in moments of crisis, and the intelligence services should have a responsibility to retain their focus on their missions and not be pressured by the committee into adopting new objectives. Another critical issue of oversight is the balance between committee independence and criticism on the one hand, and the maintenance of a working relationship between the committee and the intelligence agencies on the other hand. At the same time the committee must avoid becoming the protector or advocate for the intelligence services.

A parliamentary intelligence oversight committee's authority is a constant reminder to the intelligence services to perform their task correctly and assures the public through the members of the committee that the services are not left to their own devices. As a general rule, intelligence services – under such procedures as the parliament and government may establish, and consistent with applicable authorities and duties, including those conferred by law upon the executive, legislature, and judiciary, to protect sources and methods – should:

- Keep the parliamentary oversight committee informed concerning intelligence activities, including any significant anticipated activities;
- Upon request provide the parliamentary oversight committee any information or document in the possession, custody or control of the service;
- Report in a timely fashion to the parliamentary oversight committee information relating to intelligence activities that are illegal or improper, and corrective actions that are taken or planned.

9. Parliament plays a role in the appointment of the Director in, for example, US, Belgium, Australia and Hungary. See Born and Leigh, 2005, pp. 34–35.

Legislative oversight has to be determinedly non-partisan and discreet. Experience shows that if the members are trustworthy, services will be honest and frank with them. The oversight committee should be more inquisitorial than adversarial. Access to information will increase as confidence grows. The question of competence is more complicated. By its very nature, intelligence is governed by qualities that are unique and are not always easily comprehended by outsiders. Parliamentary involvement with intelligence is also affected by the nature of parliamentary work. Competing pressures and responsibilities mean that few legislators can devote the time needed to give them real intelligence expertise, which means in turn a reliance on well-qualified staff. The committee might want an investigator who has even wider access. It should also broaden the range of oversight beyond the intelligence services to users of intelligence. Hearings should be fair. Those mandated with the oversight have to make it clear that they can be trusted with sensitive information and can produce reports that are thorough, focused and rigorous, yet in no way compromising to the nation's security.

An important aspect of the parliamentary committee's work is that through their debates, hearings and reports, legislators can make intelligence more transparent and more visible to the public. They can heighten public awareness. A further way to achieve transparency is through questions put to the Minister responsible.

*Judicial Control and Supervision*

An intelligence service is not above the law, and sanctions must be provided for by law. If there are no enforcement measures for accountability, there is no democracy. Under the rule of law, the activities, functions, and authorities of intelligence services cannot extend beyond those that are necessary for protecting the democratic, constitutional order. Constitutional order includes the catalogue of fundamental freedoms and rights, and effective measures to protect those rights against any violation. No intelligence service can arbitrarily undermine those rights and freedoms; if it does, it threatens the constitutional order instead of protecting it.

The law must regulate intelligence activities and establish procedures to guarantee proper execution, protection and transparency. Without a legal framework, legislative oversight and executive control and accountability would have no reference point and their work would make little sense.

Intelligence is essential to informed decision-making. However, particular measures employed to acquire domestic intelligence – apart from being responsive to legitimate governmental needs – should be conducted in a manner that preserves and respects established concepts of privacy, civil liberties, and civil rights. It is here where control and supervision is most required. Judicial control and supervision must set limits intended to achieve the proper balance between protection of individual rights and acquisition of essential information (Born and Leigh, 2005, pp. 37–42). Collection procedures should normally be approved by the highest judicial authority, usually the attorney general. Those procedures should protect constitutional rights and privacy, ensure that information is collected by the least intrusive means possible, and limit the use of such

information to lawful governmental purposes. Hence, operations of the domestic intelligence agency should be subject to judicial examination after the event by a tribunal to investigate complaints about the service from members of the public and to review the warrants issued by the Minister.

For judicial control and supervision to be effective, the attorney general should:

- Receive and consider reports from the services;
- Report to the Minister responsible, the Prime Minister or the President in a timely fashion any intelligence activities which raise questions of legality;
- Report to the Minister responsible, the Prime Minister or the President decisions made or actions taken in response to reports from the services;
- Inform the Minister responsible, the Prime Minister or the President of legal opinions affecting the operations of intelligence services;
- Establish or approve procedures for the conduct of intelligence activities.

Such procedures should ensure compliance with the law, protect constitutional rights and privacy, and ensure that any intelligence activity within the country, or directed against any citizen, is conducted by the least intrusive means. The procedures should also ensure that the use, dissemination and storage of information about citizens acquired through intelligence activities is limited to that necessary to achieve governmental purposes.

*Informal and Indirect Supervision by the Public*

Civil society organisations − NGOs, lobbies, pressure and human rights groups, political parties, professional, cultural, and other advocacy or special interest associations − and the media, can perform a useful function of scrutiny of intelligence services. Informal supervision by the public can help ensure that the objectives of an intelligence service are beneficial for the society as a whole, rather than for a specific political party or an elite group of individuals. Civil society organisations can play a role in articulating the demand for accountability of the government and can draw public and political attention to infringements of civil liberties and human rights. Lobbies, advocacy and interest groups can serve to educate and inform the public, and to challenge or support government policy decisions.

Since a well informed citizenry helps to make the government responsive and accountable, a structural factor that may facilitate supervision and transparency is the possibility that information about intelligence activities becomes available after a certain period of time, such as through 'freedom of information' legislation (as in the US and Canada), and rules on release of classified materials after a set period of time. This possibility of 'delayed transparency' may facilitate democratic control.

It is similarly important that the threats to the country are outlined in a concrete way and that the public is educated about these threats. This will result in

an increase in public support for intelligence services, as well as greater control and supervision.

Human rights organisations can effect change to intelligence services through providing victims of intelligence services with access to information from security files, through litigation, and efforts to educate the public about intelligence issues. While they should stay informed about intelligence and civil liberties issues and monitor changes in the laws so that they can assert pressure on parliament, human rights groups also have a responsibility to educate the media about the complexities of intelligence issues, urge them to cover public debates and produce in-depth articles and commentaries that can enhance public understanding and awareness about intelligence.

## Conclusion

In conclusion, it is found that the prerequisite for effective control, accountability, and oversight is intimate knowledge of the role, mission, and functioning of the intelligence services. Such knowledge and understanding is even more essential for any reform of intelligence services in order to make them more efficient and more legitimate.

In particular, more efficiency in intelligence is needed to enhance national security against the growing number and diversity of risks, dangers, and threats, and to promote stabilisation of the strategic environment. It is also essential in the quest for intelligence on security issues that governments will have to pursue and to enable better informed policy-making, decision-making and effective crisis-management. Finally, a greater efficiency of intelligence is needed to increase the relevance of national intelligence to the working of international institutions, and for international action in the interest of security, justice and humanitarianism.

More efficiency can only be achieved if the role and function of intelligence is understood by the state's institutions and the public, and if intelligence is used to its best effect by the government. In this respect, a greater legitimacy of intelligence is needed to gain more respect and trust from the general public and representatives and to make intelligence a permanent part of the nation-state. In this regard, it is necessary to make national interest and the prevention of risks and dangers the *raison d'être* of the intelligence services and to enable more international intelligence exchange and sharing, which is a necessity for the international community since international action is no more cohesive than the intelligence assessments that underlie it. Finally, greater legitimacy is important to restrain intrusive methods of intelligence collection for purposes not geared to national security or support of the international community.

# PART II

# Reforms in Eastern Europe

*This page intentionally left blank*

Chapter 3

# Control and Oversight of Security Intelligence in Romania

*Larry L. Watts*

## Introduction

According to a 2002 poll, a majority (60 percent) of the Romanian population believed that their intelligence services – in particular the SRI (*Serviciul roman de informatii* – domestic security intelligence) and the SIE (*Serviciul de informatii externe* – foreign intelligence) – had been 'transformed into democratic institutions on the western model' (IRSOP, 2002).[1] 52 percent believed that the services were serving national interests in a politically-neutral fashion as opposed to the partisan aims of the sitting government (32 percent), and 55 percent had a generally 'good opinion' concerning their performance. 73 percent of the population believed that the services did not have too much power, and half of those believed they had too little power, while 74 percent believed that intelligence specialists remaining from before 1989 – about 15 percent of the SRI and 18 percent of the SIE at that time – should be retained. Periodic polling by other agencies regularly ranks the SRI just behind the church and the army, and ahead of the government and police, in terms of public trust (C.D., 2002).

The strength of this public approval came as a shock for the intelligence services which were conditioned by their overwhelmingly negative portrayal in Romanian print media.[2] These polling results indicate a veritable revolution of public attitudes since 1989 when the Department of State Security – the dreaded *Securitate* – was not only considered an institution whose repressiveness rivalled that of the Soviet KGB and the East German Ministry for State Security (*Ministerium für Staatssicherheit – Stasi*), but was also commonly perceived as the primary villain responsible for the 1,000 casualties of Romania's December 1989 Revolution. The reasons for this shift are several, including the timing and degree

1. The poll results are from a March 2002 poll. The results were presented on the national television station during a prime-time discussion with the SRI and SIE directors, Romanian journalists, and American consultants from the US-NATO Committee, 23 March 2002.
2. The same lack of balance was evident in foreign treatments of post-89 Romanian security intelligence. Baleanu, 1995 and 1996, and Deletant, 2001.

to which control and oversight of the intelligence services were introduced, observable improvement in the effectiveness of parliamentary oversight bodies, the continued existence of regional instability and risks along Romanian borders, public perception of the main factors responsible for domestic stability within the country, and the public debate initiated by the services prior to their wide-ranging reform in 2001–2002.

The Romanian intelligence community consists of six services and ministerial substructures that are specifically charged with covert intelligence collection: the SRI, SIE, the Guard and Protection Service (SPP) – concerned with the protection of Romanian and foreign VIPs – the Defence Ministry's Directorate of Defence Intelligence, the General Directorate of Intelligence and Internal Protection (DGIPI) of the Interior Ministry, and the Justice Ministry's General Directorate for Protection and Anti-Corruption (DGPA).[3] The SRI, as the principal intelligence service responsible for internal security, is the object of this study. After providing some historical background to current reforms and the central preoccupations that drove them, this chapter examines the various control and oversight mechanisms that have been developed over the SRI. Particular attention is given to the state of executive control and coordination, legislative oversight, judicial oversight, public oversight, and international cooperation and oversight of domestic security intelligence.

## Historical Background

The sudden and violent nature of Romania's revolution greatly conditioned its subsequent intelligence reform process. Unlike Poland and Hungary, it did not overthrow communist dictatorship as the result of long negotiation and consensus-building and, thus, had much less continuity in security intelligence structures and personnel.[4] Unlike Czechoslovakia, the violence of its revolution and the perceived negative role played in it by the security apparatus made the severe curtailment of its powers, and the firm control and effective oversight of successor services central and immediate priorities.

On 21 December 1989, Ceausescu retreated before an angry populace on national television, marking the end of his dictatorship. The next day, in the midst of widespread fire fights that lasted until the dictator's execution several days later, the new authorities of the Council of the National Salvation Front (CFSN) shut down the wiretapping and recording centres, opened them to public inspection, and outlawed the interception of private communications – a provision that remained in force until July 1991 (MND, 1990). On 26 December, the *Securitate* was

3. DGIPI and DGPA were reorganised in 2005. The Special Telecommunications Service (STS) is often erroneously cited as an intelligence service but is occupied with critical communications infrastructure protection and has never had covert intelligence gathering responsibilities.
4. For a comparative regional look at intelligence reform see Watts, 2004; Born, Johnson, Leigh, 2005.

transferred from the Interior Ministry to an unsympathetic Defence Ministry, simultaneously losing all of its law enforcement powers of arrest, detention and interrogation (Decree No. 4, 1989). Four days later, on 30 December 1989, the *Securitate* was entirely dismantled (Decree No. 33, 1989).

Within a month of the December 1989 Revolution, the former fourth Directorate for Military Counterintelligence, the fifth Security and Guard Directorate, the sixth Criminal Investigations Directorate, and the Deception Compartment were all dissolved, as were the Bucharest Security Unit (*Securitate* Inspectorate for the Municipality of Bucharest – ISMB) and the territorial units of Brasov, Cluj, Timisoara and Sibiu. These structural changes resulted in 2,859 redundancies, while an additional 3,637 personnel were dismissed from the central units and country structures. The uniformed paramilitary *Securitate* troops and the Airborne Unit – a total of 2,899 personnel – were transferred to the Defence Ministry (and later to the Interior Ministry), and 449 communications and software technicians were transferred to a transmission unit within the Defence Ministry (Magureanu, 1990; BBC, 1990).

Systematic vetting was carried out by the Defence Ministry's chief of personnel. By the end of January 1990, over 10,000 of the 15,312 personnel employed by the *Securitate* were excluded from the personnel pool that provided the SRI with its manpower. Of the 4,944 personnel initially judged suitable for the new service at the end of January, another 806 were cut on 1 February 1990, leaving a pool of 4,138 vetted personnel – about 28 percent of all former *Securitate* personnel as of 22 December 1989 (SRI, 2002a).

While the need for intelligence services was generally recognised by the new leaders, they were not anxious to risk duplicating the *Securitate* experience by quickly reconstituting a security intelligence agency. Nor did the public trust the new authorities not to abuse whatever executive power they acquired. This fear and mistrust were reflected in the 'hands off' attitude of central authorities towards wiretapping during the critical first 18 months of Romania's transition. Although an understandable reaction to the years of *Securitate* intrusiveness so fresh in the Romanian memory, the exclusion of such a basic intelligence collection technique denied authorities the ability to prevent or even foresee domestic crises and external provocations. This critical intelligence gap was magnified by the lack of public order bodies, which had been dismantled as symbols of repression. Together, their absence left the fledgling institutions of government extremely vulnerable, and uncontrolled demonstrations repeatedly culminated with the storming of central government buildings during January and February 1990. When communications interception was finally authorised in the July 1991 National Security Law, it was restricted in six separate articles (Law No. 51, 1991).

A violent ethnic clash in the Transylvanian town of Tirgu Mures on 19–20 March 1990 again caught central authorities off their guard. The potential for igniting broader ethnic conflict that could result in national disintegration was strongly sensed rather than fully comprehended in Bucharest, as the parallel degeneration of Serb-Croat relations in the neighbouring Socialist Federated Republic of Yugoslavia had not yet led to the break-up of that country. The Tirgu

Mures incident, which branded Romania as a potential ethnic 'powder keg' throughout the first half of the 1990s, underscored the perceived urgent need for a domestic security service to provide forewarning and to allow for contingency planning.[5] In the immediate aftermath of Tirgu Mures, a military advisory team headed by Col. Ioan Talpes was charged with drawing up the decree that would establish the new service.[6] Borrowing basic structural and organisational elements from US, Canadian, and European intelligence models, Decree No. 181 of 26 March 1990, which created the SRI, also reflected the preoccupation with domestic instability. Article One established that the SRI's mandate was:

> to gather data and information pertaining to the activities carried out by espionage services, extremist and terrorist organisations directed against Romania, by elements intending to organise and carry out diversions and criminal attempts, and pertaining to actions directed at undermining the national economy and destabilising the rule of law.

Even before the parliament came into existence, parliamentary oversight was designated in Article Two as an aim of first priority. It stipulated that the SRI was 'responsible for all of its activities' to the ad hoc legislative body – the Provisionary Council for National Unity (CPUN), formed in February 1990 – and then to parliament, following the first elections scheduled for 20 May 1990. The SRI Director was obliged to 'submit regular reports regarding the main issues resulting from its specific activity and directly answer questions regarding the service' to the legislature; and the CPUN and future parliament were expressly authorised to set up specific 'committees for the oversight of the SRI's compliance with constitutional principles and norms, and the fundamental rights and liberties of citizens' (Decree No. 181, 1990). Article Three established the SRI as a state body subordinated to the President, empowered the CPUN to approve its organisational structure, and set down that the personnel status of SRI officers would be governed by the Law on the Status of Military Personnel (a new version of which was passed five years later). Article Eight set up a public relations department and empowered the President to authorise the SRI to establish relations with foreign counterparts.

In order to be effective as soon as possible, the SRI relied substantially on former *Securitate* officers, which formed 60 percent of the SRI's personnel in 1990, together with young officers and command personnel from the Defence Ministry. Subsequent vetting and turnover reduced the presence of ex-*Securitate*

5. Tirgu Mures had many earmarks of a hostile intelligence operation, from the infiltration of agent *provocateurs* to the depiction of the brutal beating of the ethnic Romanian Mihai Cofariu on the front page of the Washington Post as that of an ethnic Hungarian beaten by Romanian extremists.
6. The team included Col. Mihai later made first deputy director of the SRI, and two police officers, Eugen Donose, a legal expert, and Alexandru Kilm, an anti-terrorist expert. Donose and Kilm became head of the SRI justice division and chief of its Anti-Terrorist Brigade, respectively. Talpes was named the President's National Security Advisor in July 1990 and SIE Director in April 1992.

personnel to less than 36 percent by 1994, and then to about 20 percent by the end of the decade (Magureanu, 1994). This percentage dropped to 15 percent during 2001–2002, with more than two-thirds of SRI central and territorial unit chiefs appointed since the spring of 2001 (Timofte, 2002a), and to less than 6 percent by 2007. Over 6,000 of the 6,800 personnel originally comprising the SRI in March 1990 have since left the service while new recruits have replaced them, lowering the average age of SRI manpower to 37 years (Timofte, 2002b).

Although uniformly ridiculed by the political opposition and its sympathisers, a serious effort was made to identify and punish perpetrators of the revolution's casualties (Deletant, 2001, pp. 212–216). The first trial, broadcast almost in entirety on television, was initiated on 27 January 1990 against the former Interior Minister and three senior members of the Communist Party central committee. A second trial commenced two weeks later against 22 *Securitate* and Interior Ministry militia defendants from the headquarters established in Timisoara in December 1989. By August 1990, charges had been filed against 1,456 alleged perpetrators, of which 834 were resolved.

Although 687 of the accused could not be tried because of lack of evidence, the 147 that were tried included nine generals, 34 *Securitate* officers, 47 officers and 6 non-commissioned officers from the Interior Ministry, three officers, one non-commissioned officer and 3 soldiers from the Defence Ministry, and 44 civilians – of which 33 were former state and party leaders. Almost all – 134 out of 147 – were held in detention prior to and during trial. As of 2001, the trials of 79 were concluded, 30 had received prison sentences, seven were acquitted, 15 were undergoing further investigation, one was given amnesty, and 69 were in the appeal process. The public nature of the trials did much to debunk the myth of an all-powerful *Securitate*.

One of the primary obstacles in realising all of the benefits of extensive personnel renewal was the SRI's first Director, Virgil Magureanu, who served from 1990 to 1997. Magureanu plotted with known Soviet agents when Moscow was still under anti-reformist leadership and concealed his own *Securitate* background from Iliescu when he was named to the post in March 1990, thereby compromising the effort to fully break with the past and perpetuating the old institutional mentality within the newly-restructured organisation. Consequently, the SRI remained isolated internationally until the mid-1990s (for example, with NATO's Office of Security preferring to conduct its relations with the SIE rather than the domestic security intelligence SRI before 1997).

### *Political Neutrality*

Just as Ceausescu's centralisation prompted Romanians to choose a semi-presidential system which split executive power between a President and a Prime Minister, the politicisation of the security sector created a similar preoccupation with the political neutrality of the military and security services. The non-partisanship of military personnel is thus embedded in Decree-Law No. 81 of 30 December 1989; In Article 26 of the 1991 National Security Law, which stipulates

that intelligence employees 'cannot be members of a party or of any organisation with a political or secret character and cannot be employed for political aims'; In Article 37(3) of the 1991 Romanian Constitution; In Section 3, Articles 28 and 29 of the July 1995 Law on the Status of Military Personnel; and in Article 4(1) of the 1996 Law on Political Parties (Law No. 51, 1991; Diaconescu *et al.*, 1996, pp. 105, 282–283 and 468).[7]

The SRI Law of February 1992 underscores political neutrality in several articles including the SRI oath (Law No. 14, 1992). To this end, Article 24 stipulates that the first Deputy Director and all other Deputy Directors, which have the rank of Government State Secretaries (Deputy Ministers), are appointed not by the party-based government but by the President.[8] Article 36 reiterates the National Security Law prohibition against membership in political organisations and against behaviour with a political aim, further specifying that:

> the SRI does not undertake any action which promotes or damages the interests of any political party or physical or legal person, with the exception of those whose activities contravene national security.

In general, there have been few complaints of the SRI as an institution behaving as a partisan political police – and all of those have been amply covered in the press. This does not mean that the SRI has been devoid of serious politicising influences. SRI Director Magureanu displayed a strong penchant for playing an independent political role throughout his tenure, on several occasions stepping outside the bounds of the law, for example, the partial publication of his own *Securitate* file in order to pre-empt media revelations regarding his background in 1992, and in his public stance against the candidacy of Ion Iliescu during the 1996 election.[9] Immediately after he was dismissed as SRI Chief in April 1997, Magureanu started his own political party – the National Alliance (AN) – substantially composed of other ex-*Securitate* officers. Obligatory vetting before the 2000 elections indicated that various AN parliamentary candidates were either ex-*Securitate* officers or *Securitate* informers (Cotidianul, 2001a).

Another sort of politicisation was manifest under the administration of President Emil Constantinescu during 1997–2000. Immediately after the revolution the new leadership reached an understanding that whereas the intelligence service Directors would be politically-appointed from outside the services, their Deputy Directors would be professional appointees. In 1997, for the first time since 1989, party politicians were appointed to operational Deputy Director posts within all of the services (including the STS), resulting in diminished expertise among the

7. Constitution Articles 80(2) and 84(1) also require the president to be non-partisan and to act as a mediator between the government and non-governmental sectors of society.
8. In this respect, it must be noted that the president, according to the Romanian Constitution, renounces party affiliation upon election.
9. When Magureanu left the service both the original and the microfilm versions of his personnel file disappeared as well.

leadership and the inflation of non-professional personnel at other levels.[10] For example, National Peasant Party Christian Democratic (PNTCD) member Mircea Gheordanescu was named first Deputy Director of the SRI, while both PNTCD and National Liberal Party (PNL) members were named to the SIE (Constantin, 2002, pp. 37, 62, 77).[11]

Restoring the status quo ante following the December 2000 elections required personnel cuts of between 10 and 20 percent (STS, 2002a and 2002b).[12] The new SRI Director, Radu Timofte, had been a member of the Senate's Defence, Public Order, and National Security Oversight Committee since its founding – heading it in 1992–1996 and again in 2001 before his appointment. One indicator of this political neutrality was the cooperation and support that the SRI lent to the National Anti-Corruption Prosecutor (PNA) – an independent entity set up in July 2002 and then merged into the General Prosecutor's Office in 2005. The SRI helped to set up a sting operation in December 2002 (the 'Pavalache Affair') that netted the principal economic counsellor to the Secretary General of the government eliciting a $4 million bribe (Dobran, 2002). The counsellor was also one of the largest contributors to the ruling party's campaign fund.

*Electronic Surveillance*

Electronic eavesdropping, believed to be extensively practiced by the *Securitate*, was another central preoccupation of the new political leadership. Prior to 1990, Romanian telecommunications were limited to the centrally controlled fixed line telephone system which was installed by the International Telephone and Telegraph Company (ITT) in the 1930s. Wiretapping and recording were thus a simple matter of identifying target lines and rerouting them through six central offices in Bucharest and a dozen other offices in the central telephone exchange buildings in Bucharest. On 22 December 1989, these centres were shut down. Following the revolution there was virtually no control of new technologies for clandestine surveillance that entered the country. This became increasingly problematic with the rapid introduction of the even more vulnerable cellular phone technology during the early and mid-1990s.

The 1991 National Security Law attempted to address the issue by establishing restrictions and sanctions ranging from 1 to 7 years imprisonment for illegal possession, fabrication or use of surveillance equipment (Article 19), and against surveillance without or exceeding legal warrant (Article 26). Similar sanctions were stipulated for public use of ancillary information regarding the

10. Deputy Director posts were envisioned to be the most senior position for active service intelligence officers.
11. Gheordanescu was a non-professional political appointment to what had previously been a professional intelligence leadership post, even if he did publicly renounce his party affiliation after his posting.
12. Employment of political friends and family in the SIE inflated personnel of the medical branch to more than a quarter of the entire service under Director Catalin Harnagea.

private life, honour or reputation of citizens gathered in the course of legal surveillance (Article 21). However, allegations of illegal surveillance by the SRI under Magureanu during 1990–1997 and again under his successor Costin Georgescu during 1997–2000 were commonplace and, in more than one instance, credible (Deletant, 2001, pp. 215–216 and 231–237).[13] In contrast, since 2004 most allegations of illegal surveillance by the services were made by politically-influential economic interests under investigation for major corruption and espionage (e.g. ROMPETROL boss Dinu Patriciu and director of the ZIUA, GARDIANUL and AVEREA newspapers, Sorin Rosca Stanescu, for manipulating the Stock Exchange, and Communications Minister Zsolt Nagy and former Vice Prime Minister Codrut Seres for fixing public bidding in the energy sector).

Enforcement of surveillance restrictions has been poor, primarily, but not only, regarding unauthorised surveillance by private security companies and economic interest groups. This is partly the result of a weak and vulnerable justice system and partly due to public and media confusion as to what constituted punishable invasions of privacy, legitimate activities in the service of freedom of information, and justifiable disclosures in the public interest. While there have been credible allegations of illegal wiretapping, the issue as to the responsible parties is complicated by repeated cases where one agency or individual has misrepresented itself/themselves as an SRI (or SIE) authority in order to carry out illegal surveillance activity (Deletant, 2001, pp. 232–233).[14]

The National Security Law categorised the illegal interception of communications as a national security threat. According to the 2002 SRI report on *The Danger of Illegal Communications Interception*, such activities are primarily 'aimed at information that damages national security' with most illegal wiretapping oriented towards 'comprising and blackmailing' entities and individuals 'by undermining the constitutional rights of free communication and protection of one's image and privacy' (SRI, 2002c). The Romanian Penal Code also criminalises the violation of private communications, while Article 7 of the SRI Law obligates the service to monitor and counter attempts to illegally 'fabricate, possess or use means of intercepting communications, as well as the collection and transmission of secret or confidential information' (Law No. 14, 1992).

Unfortunately, this legal framework has failed to discourage the phenomenon. According to media and SRI sources, during 1992–2001 'the number of cases of illegal telephone wiretapping and of the interception of other types of communication in which security firms and telephone company employees are implicated has undergone a worrying increase' (Mediafax, 2002). In the opinion of the SRI, the legal framework is 'incomplete, obsolete, ambiguous, confused and maladapted to technological progress and to the new forms which illegal interception activities have taken' (SRI, 2002c). Principally, the law fails to (1)

13. The opposition considered the overwhelming majority of such allegations credible.
14. Such 'cover' is used by those pursuing other illegal activities as well. For example, the son of the head of personnel in the DGIPI caught running a drug trafficking ring in December 2002 had license plates falsely suggesting SIE affiliation (B 01 SIE), Levant and Boeru, 2002.

identify specific technical means of communications interception; (2) clearly establish under what conditions their use constitutes an infraction; or, (3) firmly impose interdictions or obligations on economic agents which sell them. The weakness and inconsistency of the legal system is also clearly at fault. As the SRI report notes:

> … because of the various interpretations which can be given to the legal provisions in this domain, criminal investigative and judicial bodies have adopted contradictory solutions in cases which the SRI has presented to the Prosecutor's Office, the majority being acquitted. Most of the time, they have acquitted the accused because they considered that the acts committed did not present a danger to society (2002c).

This failing created a favourable environment for the further proliferation of the phenomenon. An SRI-led campaign begun in 2002 to regulate interception equipment and private security firms had been seriously curtailed by 2007.

## Executive Control and Coordination

In order to insulate the service from party struggles and politicisation, and render its use against political opponents more unlikely, it was decided not to subordinate the SRI (or the SIE, the SPP, and, later, the STS) to party-based government. In keeping with plans to create a semi-presidential system where the President held primary responsibility for national security, public order and foreign policy, the SRI was established in March 1990 as 'a central body of the state administration…directly subordinated to the CPUN's President and, after the 20 May 1990 elections, to the President of Romania' (Decree No. 181, 1990, Article 3).[15]

The Supreme Defence Council of the Country (CSAT) was subsequently charged with organising the SRI and coordinating its activities (as well as those of the SIE and SPP), and assisting in its tasking (Diaconescu *et. al*., 1996, pp. 264–267 and 499). CSAT's twelve voting members include the President (chair), Prime Minister (vice-chair), the Ministers for Defence, Interior, Foreign Affairs, Justice, Industry and Finance, the Directors of SRI and SIE, the Chief of the general staff and the President's National Security Advisor.[16] To be effective, coordination must be active. Although the CSAT is obliged to meet at least quarterly, it has met almost once every six weeks over the last eleven years.

---

15. Article 4 stipulated that active service officers could not be appointed director of the SRI, while Article 8 created the precedents for public and international outreach by establishing a public relations department and granting the president the power to authorise the SRI to establish relations with foreign counterparts.
16. The Bulgarian National Security Council, Czech State Defence Council (1990–1993)/Security Coordinating Council (1993–1994)/Board for Intelligence Activities (since 1994), and the Slovak State Defence Council all have similar membership, as do most other coordinating councils.

The membership of the CSAT reflected the fact that state institutions and government ministries were all primary consumers of the intelligence product. It was also intended that joint coordination and tasking by state and government institutions would further diminish the possibility of the service being used for partisan interests by either the government or presidency. Several Prime Ministers (e.g. Petre Roman 1990-1991, Adrian Nastase 2001-2004, Calin Popescu Tariceanu 2005-2007) resented the service's ability to control government activities and sought either to transfer it to their authority or severely limit its powers vis-à-vis government ministries. Since 2001 SRI liaison officers attend weekly cabinet meetings at government request, with tasking reserved to the presidency and CSAT. In 2006 President Traian Basescu ended suspicions of political partisanship by appointing opposition PSD member (and Chair of the Senate's Defence, Public Order, and National Security Oversight Committee) George Cristian Maior as SRI Director.

**Legislative Oversight**

Although the March 1990 SRI decree stipulated legislative oversight, the ad hoc CPUN was primarily concerned with preparing Romania's first free election in over half a century, making its oversight of the SRI perfunctory at best. After the May 1990 elections, a joint permanent committee for defence and public order was settled, also mandated to oversee intelligence.[17] However, competing priorities, particularly the major restructuring of the army and the reconstruction of a police force, coupled with a combined lack of parliamentary experience and intelligence expertise, kept oversight superficial on many levels throughout 1990–1992.

The lack of real oversight during this period fed public fears that the successor to the *Securitate* was not only uncontrolled but still engaged in abusive activities as a matter of course. To some degree, the public obsession with a possible *Securitate* restoration counterbalanced the drawing power of other priorities. The committee did manage to ensure that SRI Director Magureanu reported to parliament for the first time in November 1990 (Magureanu, 1990; BBC, 1990; Deletant, 2001, pp. 216–217).[18]

The ability and willingness of parliament to perform this function was bolstered by Romania's semi-presidential system. Party-dependent parliamentarians were thus overseeing a state agency subordinated to a non-party President rather than an institution under the control of the Prime Minister – the hierarchical boss of majority parliamentarians along party lines. According to polls conducted in 2002, Romanians

17. Starting with the 1992–1996 legislature, permanent committees for defence, public order and national security were settled in each chamber of the parliament, but intelligence oversight continued to be a low priority.
18. Magureanu's report, delivered to parliament on 22 November 1990, covered the status of ex-*Securitate* files, controlling and vetting of SRI staff, the prohibition against electronic surveillance, the legal framework of SRI activity, foreign espionage activities against Romania, the University Square and miner's events of June 1990, and the issue of transparency regarding the SRI.

consider that the tensions arising between the Prime Minister and the presidency because of this division of executive power are a small price to pay for the added checks and balances against the over-centralisation of power that it provides (Evenimentul Zilei, 2002a).

The National Security Law adopted in July 1991 more explicitly delineated the threats to national security which came under the SRI remit and reaffirmed parliamentary control over the services (Law No. 51, 1991, Articles 3 and 8). The December 1991 Romanian Constitution also provided for 'close scrutiny by the parliament of defence and security matters', requiring that both chambers meet in joint session 'to appoint on proposal of the President of Romania, the Director of the SRI, and to exercise control over the activity of this service' (Leigh, 2002, p. 5). After the creation of a constitutional basis, the adoption of a law for establishing and regulating the SRI was one of parliament's first priorities.

The SRI Law of February 1992 set down a more 'concrete and permanent' parliamentary oversight through a 'joint committee of the two chambers' (Law No. 14, 1992, Article 1). It also stipulated parliament's authority in naming the SRI Director based on the report of the joint committee after hearing the President's nomination, as well as the committee's control over the SRI budget (1992, Articles 23 and 42). The process of defining the structure, functioning and methods of exercising that control was delayed by Romania's second national elections in 1992 and completed in mid-June 1993 (Decision No. 30, 1993). The creation of the joint committee had a notable palliative effect on public paranoia regarding domestic security intelligence as reflected in the diminished number of front-page headlines devoted to SRI-centred scandals after 1993. At the same time, the public and the media continued to group all problems related to intelligence control and abuse under the 'SRI-*Securitate*' heading into the late 1990s.

The effectiveness of oversight is directly related to the scope of authority granted to oversight bodies and the seriousness and experience of the overseers. It is also dependent on the frequency with which oversight bodies meet, on the number of administrative and expert staffers that assist them in their work, and on the degree to which committee members are focused on the topic. Committees specialised by service tend to develop more extensive expertise than committees which must oversee other services as well. Committees that meet frequently are more effective than those which seldom convene. Committee members who serve exclusively are able to exercise more serious oversight than those whose members are compelled to divide their time and attention among multiple committees. And finally, committees that have both administrative and expert staff are more effective than those which lack the requisite staff support (Born and Leigh, 2005).

As a permanent joint committee, the SRI oversight committee meets at least once a week during the parliamentary schedule. The Committee is composed of nine members, allocated according to the parliamentary representation of their parties. SRI Oversight Committee members do not serve on other parliamentary committees. The Committee has three administrative staffers and, in December 2002, doubled its expert staff to four. The SRI Committee's responsibilities as established by parliamentary decision are to:

- Verify the Constitutional and legal compliance of SRI activity;
- Examine reported breaches and determine measures necessary to restore legality;
- Investigate citizens' allegations of civil rights abuses committed in intelligence gathering that are forwarded by either of the committees for defence, public order and national security;
- Examine and resolve other complaints regarding legal violations by the SRI;
- Hold hearings on the presidential nominee for Director and submit a report to the parliamentary plenum;
- Examine the annual report submitted by the SRI Director and submit its own report on the report to the plenum;
- Examine the budget drafts submitted by the SRI and present its own proposals and observations regarding budget allocations to the specialised parliamentary committees and the plenum for its adoption or rejection;
- Monitor the way in which the SRI uses its allotted funds from the budget and from extra-budgetary sources; and,
- Verify the legal compliance of the SRI's autonomous corporation, production companies, and health, cultural and sports institutions.

The Committee is empowered to request reports, informative notes, handwritten accounts, data and other information from the SRI, except when they involve current operations, the identities of agents and sources, and the specific means and methods employed in intelligence activities (so long as they conform to constitutional provisions and current laws.) The SRI is obliged by law to make requested reports, information, data, and SRI personnel available within a reasonable period of time. The Committee may summon the SRI Director and senior officers, and anyone else suspected of having some connection with issues under examination. It is also empowered to visit the SRI's central or territorial offices unannounced for inspection and monitoring purposes, and the SRI is obligated to grant it full access when it undertakes these inspections.

During 2001, the Committee carried out seven field inspections in the SRI's central offices and ten in territorial offices. It conducted four special investigations and held twenty-three hearings of the SRI Director and other SRI officials.[19] It also requested and received 55 reports, accounts and documents. As of result of these controls, the Committee identified the need to improve the legal framework for countering corruption and organised crime, for protecting civil rights and liberties against abusive incursions by private security agencies – particularly regarding illegal surveillance and wiretapping, and for strengthening the nation's anti-terrorist defence system.

19. Communication to author from Ioan Stan, then Chair of Committee for Oversight and Supervision of the SRI, 18 July 2002.

**Judicial Oversight**

Judicial oversight is generally limited in practice to the consideration and issuing of warrants for technical surveillance that infringe on civil rights and liberties. By requiring the approval of judicial authorities – whether judicial commissioners, prosecutors, or judges – a pre-emptive control is established. However, even in developed democracies these judicial authorities are not known for 'high rates of refusal' when warrants are requested and there appears to be little cause for preferring one legal authority over another (Leigh, 2002, p. 11). However, the judiciary has proven perhaps the most resistant refuge of former *Securitate* and communist-era militia personnel. As of 2007 there had been no lustration of its members or public pressure to improve transparency in this domain.

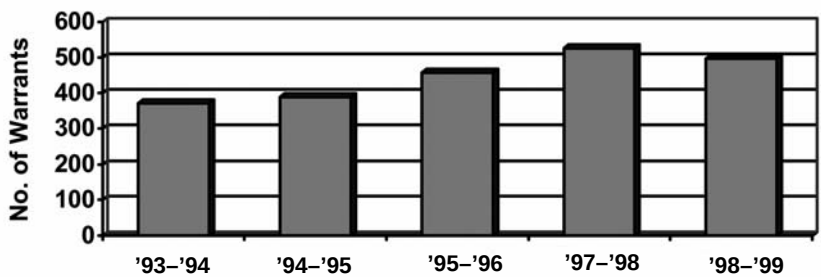
The 1991 National Security Law, which first re-empowered the SRI and the SIE to undertake technical surveillance, also stipulated judicial authorisation. Article 13 states that requests for warrants must be approved by the General Prosecutors' office and must contain details regarding the:

- Motivating threat to national security (as stipulated in Article 3 of the law);
- Category or categories of activity for which the warrant is being issued (surveillance, wiretapping, search, seizure, and so on);
- Identity of persons whose communications are to be intercepted, if known, or of the persons who hold the information, documents or objects that must be obtained;
- General description of the location where the warranted activities will be carried out, if and when it is possible;
- Duration for which the requested warrant is valid (up to 6 months initially); and
- Service empowered with the execution of the warrant.

Warrants are valid for six months, although they can be extended when cause is shown for three month intervals. The number of warrants issued annually between 1993 and 1999 in accordance with Article 13, range from 371 in 1993–1994 to a high of 526 in 1997–1998 (Stan, 2002). In 2005 warrant approval was reassigned from prosecutors to judges, although prosecutors were permitted to approve 24-48 hour warrants during weekends when judges were off-duty.

According to SRI oversight committee former Chair Ioan Stan, checking the legality and propriety of warrants and surveillance procedures is one of the most

**Table 3.1 Surveillance Warrants 1993–1999, Romania**




*Source:* Stan, 2000

frequent oversight tasks carried out by the SRI oversight committee.[20]

**Public Oversight**

The 1991 National Security Law stipulates that citizens 'who consider themselves unjustly targeted by the activities authorised in the warrant … may address a complaint against the designated prosecutor who issued the warrant directly to his hierarchical superior' (Law No. 51, 1991, Article 13). It is further stipulated that any citizen 'who considers that their rights or liberties have been broken through the use of means' employed in obtaining information 'may notify either of the permanent commissions for defence and public order of the two chambers of parliament' (1991, Article 16). Citizens may also address complaints directly to the SRI.[21] In 2001, the Committee addressed the problems raised in 142 complaints, heard 62 citizens, and conducted 11 investigations based on citizen's complaints. In several cases, SRI personnel were brought to trial.

The Romanian media has often been critical in starting internal SRI investigations and SRI Committee inquiries. At the same time, their role has not been entirely positive because of the initially low levels of professionalism characteristic of the press as a young institution, because of the predominance of economic (and other) interests, and partly because of penetration by the former *Securitate* officials. In the aftermath of the revolution, many former *Securitate* officers and their collaborators entered the press or actually acquired newspapers (Achim, 2001; Belu, 2001; and Evenimentul Zilei, 2002b).[22] In some cases, they brought with them expertise in deception, disinformation, and blackmail.

20. Communication to author, 15 July 2002.
21. By mail, in person, or through the internet via the SRI's website: www.sri.ro.
22. Since 1996, former officer Mihail Iacob was editor-owner of *Curentul*; former paid informer Sorin Rosca Stanescu was director of *Ziua*, *Averea* and *Gardianul*; former officer Sorin Ovidiu Vintu held significant interests in *Ziua*, *Academia Catavencu*, *Romania Libera* and *Realitatea TV*; *Securitate* agent Dan Voiculescu owned *Jurnalul National* and

Indeed, press blackmail was signalled as a major problem in a 1999 study of the Romanian media, and again in the international and domestic media in 2002 (International Federation of Journalists (IFJ), 1999; McAleer, 2002).[23] According to one Romanian newspaper Director, the increasing use of blackmail by the Romanian press seriously undermines its ability to hold political power accountable (Cornel Nistorescu in Voiades, 2002). Both western and Romanian observers have criticised the 'tendentiousness' (Carothers, 1996, p. 85) and 'low reporting standards' (Brown, 1994, p. 1) of the print media over the past decade.[24] In a 1999 comparative study of Albanian, Bulgarian, Croatian and Romanian press, the International Federation of Journalists (IFJ) judged the Romania print media the 'least responsible' and least professional (IFJ, 1999, p. 26).

The problematic nature of the Romanian press is well-illustrated in its portrayal of the 'Timofte-KGB' affair.[25] The media began reporting alleged links between Radu Timofte and the KGB shortly before the 2000 elections when his name was put forward as a possible future Director of the SRI. The press reiterated these allegations immediately prior to Timofte's appointment as SRI chief, demanding his withdrawal from consideration for the post (Georgescu, 2001). On the contrary, as a career soldier until the mid-1980s, Timofte was harassed by the *Securitate* after his sister immigrated to the US and then forced to resign from the army (Sima, 2001; Bucura, 2001a).

Timofte's military experience, combined with the fact that he did not have a reputation of overwhelming sympathy for the services, weighed significantly in his appointment as the first chair of the Senate Committee for Defence, Public Order and National Security in 1992. He served continuously on that committee until his appointment as SRI Director in 2001. Deemed a threat by some SRI Officers in 1993 because of his critical attitude, a report alleging a link with the KGB was forged to discredit him under the directorship of Virgil Magureanu (Oprea, 2001; Bucura, 2001b; Diac, 2001; and Ciobanu, 2001). Timofte's persistent attention to and criticism of the cover-up surrounding the 1998 *Tigareta II* affair, which involved senior political and military leaders, provoked a further elaboration of the 'evidence' during Costin Georgescu's tenure as SRI Director (Berdeli, 2001).

The press allegations prompted an extensive parliamentary investigation during which all former SRI Directors and the head of the pre-1990 anti-KGB unit were heard as well as an internal SRI investigation that uncovered the conspirators and resulted in the dismissal of seven senior officers including the first deputy Director, one division chief, and two regional heads (Belciuganu, 2001; Toma and

---

the *Antenna* TV stations; and oil magnate Dinu Patriciu held majority shares in *Ziua*, was investigated for laundering money through *Academia Catavencu*, and acquired *Adevarul*.

23. Another troubling aspect of the Romanian press was a generalised practice to 'go after' persons who demanded their right of reply or who criticised the press.
24. Both used *Romania Libera* under editor-in-chief Petre Mihai Bacanu as their example of poor journalism.
25. The *Komitet Gosudarstvennoy Bezopasnosti* (Committee for State Security - KGB) was the political police and intelligence service of the Soviet Union.

Hogea, 2001; and Stefan, 2001). Throughout the investigation press coverage was overwhelmingly prejudicial against Timofte, reaffirming the 'Timofte-KGB' linkage before, during, and in some cases even after the investigation was concluded. The same tactic and similar allegations were employed against President Iliescu in 1995–1996 and revivified in 1999–2000, including forged documents and non-existent interviews with fictitious KGB officers.[26]

Along with the external oversight exercised by executive, parliamentary and judicial organs, the capacity for internal oversight is a key development in democratic evolution. An essential corner has been turned when services develop and exercise the capacity to oversee themselves. One partial example was the internal investigation in the Timofte-KGB affair. Another example was the arrest by the PNA of the Director of RADET – *Regia Autonoma de Distributie a Energiei Termice*, the state company that provides heat and hot water to Romanian cities – and of the senior SRI Officer in league with him for corruption (Petcu and Gheorghiu, 2002). After investigating the SRI Officer for over a year, the Internal Security Department of the SRI informed the PNA of the case and turned over the results of its investigation, enabling the arrests and further criminal investigation (Tudor, 2002; Serbanescu, 2002).

*Transparency and Outreach*

Although the SRI began developing a website at the end of the 1990s, the project was moribund until 2001. The SRI website is now updated every 3–4 days (Iordache, 2002). It contains SRI Communiqués and information on the SRI, its history and attributions, education system and career opportunities, as well as major press coverage. Unclassified versions of the annual SRI report are posted on the website. Unclassified versions of special reports originally prepared for the oversight committee are also posted on the website once they are released by parliament (Levant, 2002).

The post-2000 SRI leadership identified the broader lack of security expertise related to intelligence and its legitimate functions among civil society as constituting one of the most significant challenges to the effective performance of the SRI. The problem was closely akin to the lack of civilian defence expertise that confronted political and military authorities immediately after the 1989 revolution. In order to redress this shortcoming, the SRI (and SIE) created the Higher National Security College (HNSC) on the model of Romania's National Defence College, founded in 1991 to help create a civilian defence community (Watts, 2001, pp. 604–607). The HNSC provides instruction on security and intelligence issues to public authorities and parliamentarians, other intelligence structures, civic organisations (particularly those with preoccupations in the defence and security sector), journalists, and independent analysts. It opened its doors to students in

26. This details of how this 'evidence' was manufactured were revealed in a court trial which *Ziua* lost in 1996. Emil Constantinescu simply vacated the sentence after his election at the end of 1996, so that 'Iliescu-KGB' allegations could resurface before the 2000 elections. The Romanian electorate did not find the allegations credible.

April 2002. In September 2003, the SRI co-sponsored the creation of an Information Center for the Security Community that provided public information about the security requirements and standards of NATO membership.

Magureanu's attempt to modernise the recruitment and training of SRI Officers was faulted in its conception because of the impenetrable barriers it raised between SRI personnel and Romanian society. In Magureanu's vision, modernisation required the creation of the SRI's own university – the National Intelligence Institute (NII). Recruiting for the university was then accomplished mainly through talent spotters; much like it had been before 1989, with young people of between 16 and 18 years of age brought in directly from high school. These recruits were then further educated over a standard four-year-long university programme in a 'hothouse' intelligence environment.[27] Extremely costly, the experiment did not yield the general levels of sophistication necessary for successful intelligence work or even for effective incorporation into the SRI institution. In 2001, open recruitment was introduced and restricted to university graduates, and training was modified to conform to the much shorter (less than one year) professional courses characteristic of NATO state intelligence service officers.[28] However, the NII's university-accredited departments represent an incredible drain on the SRI budget with extremely small return for the SRI.

## International Cooperation and Oversight

Intelligence sharing became an essential element of alliance cooperation with the shift of terrain after the Cold War, from interstate military conflict to combating the non-national and cross-border threats of terrorism, organised crime and trafficking in arms, persons and narcotics. Multinational intelligence cooperation, extremely rare before 1990, also provides a new realm of oversight.[29] Cooperation, joint training, and joint operations transfer expertise and experience not only in operational domains – the main focus of such cooperation – but in terms of oversight and control expectations as well. The SRI cooperates regularly and closely with NATO member state services, especially since it established a new counterterrorism department in 2002 (Iordache and Castali, 2002; SRI, 2002b). Cooperation in operations with the services of NATO states not only provided validation to SRI personnel but also increased its prestige as an effective institution operating in consonance with democracy among the Romanian population. The SRI now has bilateral institutional relationships with over 60 states.

27. There was a parallel indirect recruitment with shorter training schedules but the bulk of the SRI personnel were directly recruited.
28. Details are available at http://www.sri.ro.
29. Aside from the informal Club of Berne, almost all exceptions of institutionalised intelligence cooperation prior to 1990 belong to the Anglophone world: the US-UK 'special relationship', US-Canadian cooperation in signals intelligence, and the UK-USA cooperation which also includes Australia and New Zealand. International intelligence sharing efforts between states have increased considerably since 9/11.

Romania pioneered a number of regional intelligence cooperation initiatives. In April 2002, the Romanian presidency, the SRI, and the SIE jointly organised the first conference of NATO member and candidate member (MAP) security and intelligence services with the participation of 14 states.[30] Romania hosted a second NATO-MAP conference, with 21 states participating in September 2002.[31] In May 2002, the SRI was one of the main organisers of the annual 'Conference of South-East European Intelligence Services' outside of Bucharest, with the participation of services from Albania, Bulgaria, Croatia, Greece, Macedonia, Slovenia, Turkey, as well as Serbia and Montenegro (Nine O'Clock, 2002). This was the first meeting bringing together the intelligence services from the successor states of the former Socialist Federated Republic of Yugoslavia.

## Conclusions

While the legal framework for democratic oversight and control is robust in Romania, the weakness and vulnerability of the legal and justice system, particularly in the poor enforcement of existing laws and constitutional provisions, is still a significant obstacle to effectiveness and a generator of other intelligence-related problems. A thorough-going review of the *Securitate* and militia pasts of judicial personnel is also long overdue. On the general level, the Constitutional Court, the General Prosecutor's office, and magistrates need to become much more proactive and independent in their behaviour from governmental leadership. This is particularly evident in the realm of illegal wiretapping, especially regarding private security companies, economic agents and third parties, but the verification of intercepts by intelligence services and sub-structures also needs improvement.

Romania's semi-presidential system has proven itself capable of blocking the over-accumulation and over-centralisation of power by government executives. If anything, it should be strengthened by moving the monitoring and anti-corruption agencies as far as possible from that part of the executive that controls the finances and budget and is most closely tied to partisan political competition. Serious background checks and certifications for handling classified information should be required of all parliamentarians and cabinet members who sit on permanent and ad hoc intelligence committees or receive the intelligence product. Real sanctions should be introduced and enforced against institutional actors and leading political figures with authority over the security and intelligence domain who disregard the legal stipulations regarding political neutrality.

30. The conference was organised by the Romanian Presidency, the SRI and the SIE, under NATO auspices, and co-sponsored by the Grand Duchy of Luxembourg on 10–14 April 2002 at Sinaia. Former SIE Director Ioan Talpes was later honoured by the North Atlantic alliance for his role in creating the NATO intelligence community.
31. The second NATO-MAP conference was held on 25–28 September 2002.

Chapter 4

# Transformation of the Polish Secret Services: From Authoritarian to Informal Power Networks

*Andrzej Zybertowicz*

## Introduction[1]

Under communism the Polish secret services were an instrument of power of the authoritarian regime. They were tasked, supervised and controlled using measures that were not always based on the law. The delicate nature of the situation of the services in post-communist predicaments stems from the fact that once the old regimes disappear and before the new regimes are fully established, a vacuum of supervision and control arises. The old informal (yet largely effectual) measures of supervision are gone, and new democratic measures can emerge, stabilise and ultimately reach a desired level of performance, but only after a long and painstaking process.

The post-1989 history of the Polish secret services abounds with scandals, leaks, falsifications, manipulations, and actions of dubious legality and utility. The services were not only accused by various politicians, the media and independent spectators of disrupting or interfering with the political activities of individuals or organisations, but they were also accused of organising and/or suppressing political parties, initiating various media campaigns, spreading slanderous rumours, inspiring and/or hindering legal arrangements and initiating dubious economic activities (like manipulating the Polish stock market). The services were charged with the unlawful infiltration both of left and right wing political groups, bringing about the downfall of three Prime Ministers, one Deputy Prime Minister and numerous minor figures, not to mention unlawful intervention in all three presidential campaigns.[2]

---

1. The author is grateful to Daniel Wicenty and Marcin Spławski for their help and comments on this chapter, which draws heavily on research presented in a book co-authored with Maria Łoś (Łoś and Zybertowicz, 2000). The information in this chapter refers predominantly to the prevailing circumstances up to 2002, the year that it was written.

2. For example, AMC 1996; Barański, 1997, 2001; Biernacki, 2002; *Myśl Socjaldemokratyczna*, 1998; Jakimczyk, 2003b; Kosobudzki, 1998; Łoś and

A key point is the fact that although such accusations were uttered by prominent politicians,[3] developed in the most reliable print media[4] and although some investigations were launched (Indulski, 2003; Ordyński, 2000a, 2000b; Marszałek, 1999b; Rusak, 2003), convictions were made only in minor cases.[5]

In July 2001, two months before the parliamentary elections won by the post-communist parties, Zbigniew Siemiątkowski – a social democratic party MP and a Minister of the Interior in 1996, and a former government coordinator of the services who for two years directed the civilian Foreign Intelligence Agency (*Agencja Wywiadu* – AW) – stated that the reform of the services designed by him should:

> … deeply plough the structure [of the services], which was evolving for decades, [which] via informal methods captured the whole organism of the state, and up till now operate[d] at its wish beyond anybody's control and with impunity (Siemiątkowski, 2001).

In December 2001, Colonel (later to be General) Marek Dukaczewski, newly nominated Director of the Military Information Services, who had previously spent five years in the National Security Bureau of the President Aleksander Kwaśniewski Chancellery, declared that:

> [i]n Poland, during the last twelve years, there has not been a mechanism created preventing the secret services from intervening in political games (Dukaczewski, 2001).[6]

Yet, in May 2002 when parliament passed new legislation regarding the secret

---

Zybertowicz, 1999; Marszałek, 1998; Miller, 1998; Pytlakowski, 2001; Wróblewski, 1998; Zybertowicz,1999, 2002b.

3. Including members of the parliamentary commission for secret services.
4. Including the dailies *Gazeta Wyborcza* and *Rzeczpospolita*, and the weeklies *Gazeta Polska*, *Polityka*, *Newsweek Polska* and *Wprost.* See for example: Cieśla and Jachowicz, 2002; Gargas, 2003; Indulski, 2003; Jachowicz, 1997a, 1997b; Janecki, 1997; Marszałek, 1999a; Pytlakowski, 2001; Siemiątkowski, 1997; Wilczak, 2000.
5. Some exceptions are convictions of: a former UOP operative of the Bydgoszcz branch for forging a classified document (ANT, 2001; Czajkowska, 1999; Olbrot and Subotić, 1997); a deputy head of the Gdańsk branch of the UOP for misappropriation of communist secret services files related to pre-1989 activities of Lech Wałęsa (PAD, 2000; ROD, 2003); a former operative of the Poznań branch who, while being in charge of postal correspondence interception, illicitly read some private letters (including the ones sent to former Prime Minister Hanna Suchocka) and also leaked classified information (Stachowiak, 2000); a deputy chief of the Wrocław branch of the Military Information Services was given a year in prison (suspended sentence) for threatening a military prosecutor (Indulski, 2003, p. 31).
6. Such observations are not exceptional (Celiński, 2003; Dziewulski, 1997, p. 7; Hausner, 2003, p. 39; Kaczyński, 1999; Macierewicz, 2002, p. 13; Miller, 1998).

services,[7] rather than explaining the scandals and taking legal measures against those responsible and thus promoting accountability, the Polish public was offered only a quasi-reform of the services. It deserves this label because, among other things, it did not meet the objectives of its own designers. According to their declarations (SLD – *Rada Krajowa*, 2001), the two most important secret service organisations, the civilian Office of State Protection (*Urząd Ochrony Państwa* – UOP) and the Military Information Services (*Wojskowe Służby Informacyjne* – WSI), both covering foreign and domestic intelligence tasks, were to be dissolved. In their place two new organisations were to be established: the Agency for Internal Security (*Agencja Bezpieczeństwa Wewnętrznego – ABW*) and the Foreign Intelligence Agency. However, although the two new agencies were formed, the military services escaped virtually unchanged. The undercover community has once again proven that it can resist reform projects initiated by politicians (for example, Paradowska, 2002, pp. 25–26). Only in May 2006, the lower house of the Polish parliament (the *Sejm*) passed laws that liquidated the controversial WSI and set up new military intelligence services (The Warsaw Voice, 2006).

In this chapter, the notion of secret services refers to all state institutions, that are officially authorised to collect, process and disseminate information which with the help of covert methods (compare Born, 2002). The services also have the capacity – which is sometimes granted semi-legally[8] – to secretly influence or manipulate institutions, organisations and individuals.[9] This chapter will not deal with the important related issues such as public police and access to secret communist-era files in the archives of the services. Important as they are, these issues deserve a separate analysis.

Until 2006 Poland, apart from the military (WSI) and civilian services (ABW and AW), there are a number of institutions that are formally empowered to use covert methods, namely: the Military Police (*Żandarmeria Wojskowa*), the Bureau of Internal Affairs of the Border Guard (*Biuro Spraw Wewnętrznych Straży Granicznej*), the Bureau for Protection of the Government (*Biuro Ochrony Rządu* – BOR),[10] a special police unit operated within the Ministry of Finance which handles taxation crimes, and a separate section within the General Customs Office (*Główny Urząd Celny*). These institutions rely heavily on personnel trained by both communist and post-communist secret services (Pietrzak, 2000).

---

7. Statute of 24 May 2002 (Dziennik Ustaw No. 74, position 676).
8. Such 'half-legality' stems both from the tradition of the communist law and the ambiguity and very poor quality of the present legal arrangements, often criticised by experts as well as, ironically, by the MPs themselves, including the deputy speaker of the Sejm (Jankowski and Wyszomirska, 2003; Wojciechowski, 2003).
9. An example of this was the case of the so-called Lesiak group, a special team organised within the UOP and tasked with infiltration and disintegration of some of the right wing political groupings in the first half of the 1990s (Marszałek, 1998, 1999c).
10. The government in this context means top appointees in the central administration.

## The Undercover Community

In order to understand the problems arising in relations between democratic institutions and the security services in Poland, one must acknowledge the role played by the undercover community. This encompasses all the aforementioned services, as well as former employees (both of the old and the new regime) presently out of the service; those private security and detective organisations who are staffed/controlled by former (or presently under-cover) employees of the services (Skłodowski and Woyciechowski, 1997), active secret collaborators (agents) of present services, and also many formally inactive (that is de-registered) secret collaborators of communist services who are currently involved in business (Janecki and Mac, 2001; Kittel and Marszałek, 2001), the media (AMC, 1996; Sadura, 1997) and in politics (see below).

This undercover community is characterised by certain distinctive features. Foreign intelligence, which is usually perceived as an elite within the secret services, is an institution which fosters a career path different from that characteristic of contemporary civilian institutions (such as modern multinational corporations). In civilian organisations, the most talented employees plan their careers in accordance with their personal development – inter-company and inter-country upward mobility is perceived as a natural element here. By contrast, in foreign intelligence (and within the secret services in general), the success of an individual is measured by their loyalty to the institution – this is the rule by which personnel are instructed and cultivated (compare Herman, 1996, pp. 323, 329).

It seems that in the post-communist countries, members of the secret services have often been indoctrinated with a certain negligence of the law, even an *esprit de corps* described as a 'dirty togetherness'.[11] This has contributed to the emergence of an informal, self-regulating community sharing a high level of internal social capital, and a certain level of understanding and trust often overriding political loyalties, which are sometimes perceived as somewhat superficial. Thus, there is no need for an overarching conspiracy for networks of the security complex to survive and thrive. However, the undercover community is not a fully cohesive body; it is often ridden with opposing interests, but when it feels threatened by external actors it behaves in a rather uniform fashion (*Więź,* 2000).

In sum, we have a flexible network of informal interest groups with direct access to all echelons of state power, as well as with links to the criminal underworld (Biernacki, 2002, pp. 9–10). Such groups are capable of designing and successfully executing large-scale economic fraud with the intent of channelling public resources into private hands. One of the indicators of the extent and strength of these networks is that numerous crimes of this sort which are brought to light,

11. Adam Podgórecki defines dirty togetherness as 'perverse' forms of loyalty based on a matrix of different, more or less connected, partnerships aimed at making use of all formal and official structures in order to take them over for private goals, taking advantage of their administrative position and formal power' (Podgórecki, 1993, p. 99).

are rarely explained to the public despite the efforts of whistle blowers; and although formal investigations are initiated, the main culprits usually go unpunished.

What is striking is the fact that many of these crimes, achievable only with logistically complex preparations, were perpetrated in companies or institutions which had been under the so-called 'counter-intelligence protection' exercised either by civilian or military intelligence services. Such protection means that the services establish 'guardian angels' that are tasked with cultivating networks of informants within institutions under their responsibility (weapons producing firms or the Warsaw Military Technical Academy are good examples of this). It is highly unlikely that such diversified activities aiming at illicit transfers of public resources and operations involving many culprits could escape the attention of the intelligence services networks. Furthermore, in many cases, the media have documented the presence of various figures connected both to the old and new intelligence services among those suspected in the most intricate of the frauds.[12] Strikingly, numerous students of the transformation avoid showing any interest in patterns that are easily detectable by systematic readers of the Polish press and/or the Supreme Chamber of Control reports.

Another factor is the presence of the previous communist services personnel within the polity of the newly established democracies. As a result of the lustration law which was passed in 1997,[13] a number of former officers and secret collaborators of the communist secret services were identified. For example, between 1999 and 2001, in the group of judges, prosecutors and attorneys, over two hundred acknowledged their former relationships with the services. In the administration of Prime Minister Leszek Miller of the Social-Democratic Party (in office from 2001 to 2004), at least 12 people of the rank of Cabinet Cinister, Deputy Minister or an equivalent position have acknowledged such relationships (Pytlakowski, 2003a). In autumn 2003, at least seven Social-Democratic MPs have lustration procedures pending (this means that they are accused of a lustration lie, that is not revealing their true relations with communist secret services as is required by the lustration law).[14] At least four persons among the advisers of Prime Minister Miller are known to have been officers of communist and/or post-

12. Cieśla, 2003; Cieśla and Jachowicz, 2002; Cychol, 2001, 2003; Gargas, 2003; Kittel and Marszałek, 2001; Leszczyńska and Indulski, 2003; Zieliński and MNS, 2001. In regard to the Czech Republic, Slovakia and Romania, see Williams and Deletant, 2000.
13. *Ustawa z dnia 11 kwietnia 1997 r. o ujawnieniu pracy lub służby w organach bezpieczeństwa państwa lub współpracy z nimi w latach 1944–1990 osób pełniących funkcje publiczne (Dz.U. 1997 Nr 70 poz. 443)* [The Act on the Disclosure of Work For or Service In State Security Agencies or Collaboration with such Agencies in the Years 1944–1990 by Persons Holding Public Office].
14. See the website of the Representative of the Public Interest (*Rzecznik Interesu Publicznego*), that is of an office established by the lustration law. The Representative plays the role of prosecutor whenever suspecting a high official concealing her/his ties to communist secret services, available at: http://www.rzecznikip.gov.pl.

communist secret services (Butkiewicz, 2003; Olczyk and Subotić, 2002; Zalewska, 2003).

In a public speech on April 2003, Jerzy Hausner, a Professor of Economics, and then Minister of Economy, Labour and Social Policy, who in June 2003 also became Deputy Prime Minister in charge of the national economy in the Miller cabinet, stated that:

> the main sectors of the Polish economy, the ones which play a key role, are dominated by oligarchic interests of a few family clans. Some private businessmen have much more to say than ministers in charge of the sectors. It cannot also be kept secret, that in the peculiar relationships between the private business and politics, the influences of the intelligence services have an effect beyond any reasonable degree (Hausner, 2003, p. 39).

One can even maintain that the undercover community provides a beneficial environment for the pursuits of the most influential informal power groups in Poland.[15]

## Pre-1989: The Post-Totalitarian Police-State

In the book *Privatising the Police-State: The Case of Poland* (Łoś and Zybertowicz, 2000), the authors argue that Poland in the 1980s was a post-totalitarian police-state. The totalitarian state becomes a totalitarian police-state when the police agencies are no longer tools, but rather 'become the leading apparatus of the state' and the role of the party is undermined (Chapman, 1970, p. 114). Their thesis is that by the 1980s, of the three pillars on which the communist party based its power – ideology/media monopoly, the state economy and the security/military apparatus – only the third remained robust. This was due to the fact that one of the results of the Solidarity movement in 1980/1981 was the delegitimisation of communist party rule. The party lost its potential both for social penetration via local party groups and for the mobilisation of society (Dudek, 2004). The situation necessitated a re-conceptualisation of the party's relations with the secret services, whose relative power increased considerably. Łoś and Zybertowicz (2000, pp. 47–52) term the pattern of social control typical for communist states as 'regulation through infiltration'. In the 1980s, this pattern was substantially enhanced and there was a dramatic increase in the numbers of secret collaborators recruited by intelligence services, surpassing in total the large numbers that were typical of the Stalinist period. For example in 1984, over 18,000 collaborators were recruited by the civilian secret services alone (Ruzikowski, 2003, p. 116). Within this context, the character of the secret services was also to undergo important changes. No longer expected to act in the name of an ideology,

15. *Więź,* 2000; Łoś and Zybertowicz, 2000; Staniszkis, 2001, pp. 35, 79, 118; Zybertowicz, 2002a, 2002b.

these services came to be used more flexibly and pragmatically to enforce the state's policies and facilitate self-serving strategies of its elites. This stage is labelled a 'post-totalitarian party/police-state'.

The services were formidable, well-staffed, closed institutions which permeated all layers and institutions of the administrative system. The services became not only the most crucial pillar of the communist power, but also an instrument important for everyday governing practices, including the command economy.[16]

Łoś and Zybertowicz also claim that the services were not passive subjects of the wave of changes referred to as the 'systemic transformation'. The services, or to be more precise, those parts of them that were related to foreign intelligence, should instead be identified as some of the most important actors of the transformation. The services played their role through various forms of illicit privatisation of the state, economy, control apparatus, and those public spaces that used to be the communist state's domain but had been converted into private spaces or property. Under communism, virtually all state institutions that had direct contact with the West were under direct surveillance or control by one of the services. The Centres of Foreign Trade (*Centrale Handlu Zagranicznego*), one of the key instruments of the command economy which were heavily staffed with secret service agents, are a prime example of this. Therefore, it is no surprise that after 1989 the Centres were among the first state institutions to become privatised (Ogdowski, 2001). Although it is worth noting that in the late 1990s, when the more mature market instruments were implemented, the old hands were often ousted from many commanding positions (Stankunowicz, 2000).

In sum, contrary to the standard perception of the communist secret services as the 'sword and shield' of the communist party, in many Central-Eastern European countries, the services actually facilitated the dismantling of the old system.[17]

## Secret Services in a Democracy – A Dog Unleashed?

The author adheres to the view that one of the effects of the transformation in Poland (as well as in many other post-Soviet countries) is that informal elite groups, rather than democratic institutions, exert the real influence over state decision-making processes.[18] Could the services, or the security complex in general, be playing a substantial role in such a state of affairs?

16. Łoś and Zybertowicz, 2000, pp. 43–45; Zybertowicz, 1993, 1997; as far as GDR is of concern, see Childs and Popplewell, 1996; Gieseke and Hubert, 2002; Wolfe, 1992.
17. It would take another paper, if not a book, to elaborate on this issue (Łoś and Zybertowicz publications in the References and also Darski 1992; Staniszkis 1999; 2001; Williams and Deletant, 2000). One needs to add that the phenomenon at stake is very much under-explored.
18. Basiewicz and Snarski, 2003; Kamiński, 2003; Michalski, 2003; Semka, 2003; Skórzyński, 2003; Schulz, 2003.

In 1990, personnel numbers in the communist services were substantially reduced; civilian from about 25,000 to 6,000; and military from about 6,000 to 1,500.[19] The communist civilian security service (*Służba Bezpieczeństwa* – SB) was disbanded. Parts of its staff went into the superficially reformed state police. Some employees moved through a verification (vetting) procedure. Of the 25,000 former employees, 14,000 decided to undergo the procedure carried out by the newly created qualification commissions whose mandate was to exclude applicants who had previously violated the law or basic human rights. Ten thousand applicants qualified and about 3,500–4,000 of them ended up working in the newly established Office of State Protection.[20]

Qualification commissions consisted of members of parliament (including many former communists), lawyers, representatives from police headquarters, as well as members of the Solidarity Union and other deserving citizens. Yet, the verification procedure had a number of flaws:

- A large proportion of SB personnel files disappeared thus the commissions had no access to them;
- in some cases, commission members were outsmarted by experienced operatives who had a clear information advantage over their evaluators;
- some commission members feared revenge from disqualified employees;
- and the verification requirement was not applied to employees working in the observation sections, archives, communication and encrypting systems, operational techniques and passports office while foreign intelligence, and counter-intelligence operatives were treated in a very indulgent manner – many operatives of these branches got prominent positions in the UOP (Morawski, 2002; Siemiątkowski, 1998, pp. 108–9; Widacki, 1992).

It must be noted that the military services were spared any external reform and have instead reformed and 'purified' themselves through a series of organisational shifts (Maloj, 1998). Formerly separate military intelligence and counter-intelligence were combined, and, in August 1991, following the decision of the Minister of Defence, the Military Information Services were established. Until December 1995, the service operated according to secret military orders. Only the statute of 14 December 1995 on the Office of the Ministry of Defence clearly put the service under the Minister's control. The statute, however, did not regulate many legal issues relating to the activities of the military secret services, for example the WSI's freedom to apply technical operational measures. Only in 2003, when the law of 9 July on the Military Information Services was passed (see below), was the issue legally settled.

19. Piotrowski, 2003, p. 102; Widacki, 1999, p. 224; private communication with a former communist military counterintelligence officer – February 1992.
20. Miodowicz, 1996, p. 7; Niemczyk, 1994; Podemski, 2002; Widacki, 1992, 1999.
21. *Ustawa o Urzędzie Ministra Obrony Narodowej z dnia 14 grudnia 1995 r. (Dz. U. 1996, No. 10, pos. 56).*

After nearly a decade in power, the post-communist Left Democratic Alliance lost the September 2005 election. The right-wing Law and Justice party took over government and promised to carry out a 'moral revolution' in Poland which would put an end to the alleged 'Bermuda Quadrangle' of corrupt politicians, secret services operators, business people and criminals. The main political targets were post-communists who were involved in a series of money-for-influence scandals. The Law and Justice party also promised the electorate that they would deal thoroughly with the communist past and purged the secret services, removing from public life those who had taken part in the repression of the communist regime.[22] For example, in October 2005, shortly after the election victory, they fired the post-communist Director of the Military Intelligence (WSI).[23] As mentioned previously, the WSI was altogether dissolved and replaced by new services in May 2006.

*Legal Framework*

For many years, a legal framework existed only for the civilian services. The statute of 6 April 1990 established the Office of State Protection (UOP), defining its organisation, activities and objectives. However, the scandals mentioned above show that the extent to which the principles laid down in the statute were adhered to, both by the government and the services themselves, is far from satisfactory. After parliamentary victory in September 2001, the winning post-communist Social-Democratic Party found it necessary to abolish the UOP and set up two new services; this was done in the statute of 24 May 2002. The official rationale for this move was to make the services more efficient and accountable to democratic bodies (*Myśl Socjaldemokratyczna*, 1998; SLD – *Rada Krajowa*, 2001). However, the opposition claims that the actual aim was to purge the services of staff recruited after 1990 and to promote the old hands – about 400 were fired[24] who were perceived as being loyal to the previous right-wing ruling coalition which lost the September 2001 parliamentary elections. In fact, various deputy chiefs of the new civilian secret services are former operatives of the communist services. For example, General Marek Dukaczewski, the last chief of the WSI, was an officer of the communist military intelligence. Many other similar cases have also been documented.[25]

---

22. The term 'Bermuda Quadrangle' was coined by Prime Minister Kazimierz Marcinkiewicz of the right-wing Law and Justice party; (Garton Ash, 2006).
23. *NZZ*, 2 November 2005.
24. According to the Supreme Administrative Court, many discharge decisions had severe procedural flaws which make them invalid. However, for a long time the new chiefs of the services (that is of ABW and AW) refused to follow the law and re-employ those fired (D.Fr., 2002; Gottesman, 2003).
25. See the website run by some of the fired employees of the dissolved UOP, available at: http://www.republika.pl/uop12lat; the website includes full media coverage of secret service matters in Poland over the last two years. However, one should note that the process of promoting old hands into commanding positions in the UPO started

Since the beginning of the transformation, one of the tasks of the services was to screen persons in line to obtain security clearance. However, adequate legal procedures were approved by the parliament only in 1999.[26] Until then, the new agencies had a free hand to make or break political careers.

Another issue is that the internal structure of the services inherited the feature of creating *ad hoc* teams, which is characteristic of many communist organisations and allows them to diffuse accountability while providing the organisational flexibility necessary for undertaking risky and/or suspicious projects. As the scandal known as 'surveillance of the right wing political factions' demonstrated, *ad hoc* teams or structures may be created in order to pursue dubious aims and to avoid as many internal traces of their activity as possible.[27]

One needs to add a brief contextual note: is it widely acknowledged that in general the Polish legal system is haunted by systematically arranged loopholes and exemptions (Jankowski and Wyszomirska, 2003). They account for the vast amounts of discretionary authority far too often delegated to executive agencies.

*Separation of Law Enforcement and Secret Services*

Polish civilian secret services are granted law enforcement powers. They can conduct criminal investigations and have the authority to make arrests and to search homes.

In 1994, Stanisław Iwanicki, then deputy General Prosecutor, indicated that the statute of April 1990 incorrectly defined the boundaries of responsibility of the Office of State Protection (UOP), especially in regard to economic investigations (Iwanicki, 1994, p. 12). Comments also appeared, stating that the UOP section responsible for dealing with organised crime overlaps with, and substantially weakens, parallel structures in the state police (Janke, 1996, p. 13; compare Pytlakowski, 2003b).

*Division of Labour between the Services*

Responsibilities of the Office of State Protection, which operated between 1990 and 2002, included foreign intelligence, domestic counterintelligence, political police tasks (for example countering extremists groups), serious economic fraud and drug trafficking among other things. It is not surprising that the agency was

---

in 1992 under former dissident, Andrzej Milczanowski, the then Minister of the Interior, who was viewed as being 'enchanted' by the experienced communist operatives (Siemiątkowski, 1998, pp. 108–109). (Gargas, 2002; Jakimczyk, 2003a, 2003b; Łęski, 2002; Walaszczyk, 2003).

26. Statue of 22 January 1999 on Protection of Secret Information. It is worth noting that art. 42, p. 1. of the statute states that the procedures are excluded from control of the Supreme Administrative Court.

27. See for example, Ordyński, 2000a, 2000b; Marszałek, 1998, 1999a, b, c.

charged with an unnecessary accumulation of power. However, the idea of devolving the investigative powers of the civilian services – proposed by the post-communist party when it was in opposition (SLD – *Rada Krajowa,* 2001) – was eventually dropped when the reform was actually enforced in May 2002.

### *Professional Ethos*

Here, the legacy of communism is relevant. The following long-term by-products of the police-state should be taken into consideration:

- An over-reliance on covert action, understood as any activity, including the use of violence, designed to secretly influence institutions and individuals;[28]
- the destruction of the public ethic (for instance, the reduced effectiveness of delayed statutory lustration contributed to the domination of public life by people of dubious integrity and reputation);[29]
- a low level of trust in social life through constant denigration, slander, and a low level of participation in civil organisations;[30]
- the apparent insecurity of hundreds of thousands of people who had some (albeit brief) informal contacts with communist secret services and who still live in fear of the potential disclosure of their identities if an eventual lustration is conducted carelessly and vindictively; and, consequently;
- the existence of a climate of fear preventing any action that would help to clear and settle the legacy of the police-state.[31]

All of these factors seriously impede the emergence of a democratic, professional ethic in the services.

## Oversight Institutions

### *Government Tasking*

In post-Soviet Europe the secret services have been transformed under paradoxical circumstances. As observed by Kieran Williams:

> in a revolutionary situation, the institutions of security intelligence play a far more exposed, ambiguous role than they do in consolidated democratic politics. Together with ethnic minorities, they are at the centre of post-communism's moral panics and

28. On the massive infiltration of the Solidarity Movement Cenckiewicz, 2003; compare Piotrowski, 2003; Ruzikowski, 2003.
29. Grajewski, 1996; Kuczyńska, 2002; Łoś, 1995; Smolar, 2000; Zybertowicz, 1993; compare Williams *et al.,* 2001.
30. CBOS, 2002; Frączak, 2002; Frykowski, 2003.
31. Vol. II, 2003 of journal *Ius et Lex* fully devoted to this issue.

> conspiracy theories, yet at the same time they are expected to protect the people and enlighten policy-makers in a period of uncertainty and disquiet (Williams and Deletant, 2002, p. 1).

In 1994, the former Minister of the Interior from 1990–1991 and the first Director of the UOP, Krzysztof Kozłowski, declared that 'tasks for our services are formulated neither by the Prime Minister, nor the President, nor the parliament; therefore there is plenty of chaos in the work of the services' (Jachowicz and Kęsicka, 1994, p. 4). In 1995, the then Director of Military Intelligence Services announced that 'in our state there is not a centre, which would coordinate the activity of military and civilian services'. In 1996, the former Director of the UOP counterintelligence department stated that 'successive Prime Ministers could not organise their own cabinets to outline – in a systematic, not incidental manner (*sic*) – the tasks for the UOP, both short and long-term'. According to him, the services were repeatedly requested in vain for tasks to be specified (Miodowicz, 1996, p. 10). In November 2001, Jerzy Dziewulski, MP of the Social-Democratic party (at the time in power for two months), formerly a security adviser to President Aleksander Kwaśniewski, claimed that 'actually the services work beyond control. They task themselves and fulfil the tasks, also for their own needs' (Dziewulski, 2001). However, Colonel Zbigniew Nowek, chief of the UOP from 1997–2001 under the reign of a right-wing coalition, opposed Dziewulski strongly.[32]

It seems that in Poland (and probably also in other post-communist countries) the secret services have been 'reformed' before their mission was properly identified (see, Williams and Deletant, 2001). It was probably impossible to avoid outcomes harmful to democracy in a predicament where self-tasking of the services was developed over a number of years while the politicians were engaged in inter-party struggles.

*Government Oversight*

The Committee for Special Services (*Kolegium ds. Spraw Służb Sepcjalnych*) is a body of the Council of Ministers set up in line with Chapter Two of the statute of 24 May 2002. The Committee is designed as a consultative and advisory body on matters of programming, oversight and coordination of the services. At present, the tasks of the Committee include expressing opinions on, among other things, the appointment and dismissal of the Directors of the services; issuing instructions and action plans for the special services; providing recommendations for (but not the approval of) detailed draft budgets; as well as contributing to the drafting of legal acts concerning the special services. The members of the Committee also assess the execution of the statutory tasks of the special services, including the matters relating to organising the exchange of important information among the government administration organs and in the field of classified information protection.

The Committee is headed by the Prime Minister, run by a Secretary

32. Interviewed by the author in June 2003.

appointed by the Prime Minister and composed of the Minister of the Interior, the Minister of Foreign Affairs, the Minister of Defence, the Finance Minister, and National Security Advisor to the President (head of the National Security Bureau). The Prime Minister has direct supervision over the actions of the Foreign Intelligence Agency, and after consultations with the Committee for Special Services, may issue binding guidelines to the Head of the Foreign Intelligence Agency (Foreign Intelligence Agency, 2003). The sessions of the Committee are also attended by the head of the ABW, head of the AW, chief of the WSI, and chairman of the Sejm Commission for the Special Services.

When writing on the issue of government oversight in post-communist states one cannot avoid the question of the legacy of the police-state. Namely, what are the consequences of the fact that a number of figures active in political life were employees and/or secret collaborators of the secret services? Is there a critical mass of presence of such persons that makes a difference? Can we exclude that the government (and the parliament) are staffed with former and present secret collaborators of the services to such an extent that the master/slave relation becomes reversed? It seems likely that a pattern of mutual interdependence has evolved which is not conducive to the pursuit of the common good either for the services or for politicians. One should not reject outright the hypothesis that the undercover community provides a sort of nucleus of informal power networks from which formal leaders are recruited. A number of striking examples can be found to make such a guess worthy of further exploration.

*Parliamentary Oversight*

One of the legacies of the old regime is a fear of the services. In the post-1989 parliaments, a number of former secret collaborators of the communist services were identified; the process of 'wild' lustration[33] has pointed to even more; some other cases are awaiting their settlement in court via statutory lustration. Many others probably never will be made clear due to destruction or 'privatising', that is, the theft of a large proportion of communist secret service files.[34] This may be partially attributed to the insufficient vigour of parliament in scrutinising the government. Of course, party politics is another reason for the parliamentarians' complicity.

In April 1995, by virtue of the amended resolution of 30 July 1992, the Sejm Commission for the Special Services was set up. The tasks of the Commission focus on assessing legal and normative acts (bills and regulations) of a general character concerning the special services, along with providing opinions

33. The notion 'wild lustration' is used in Poland to capture a phenomenon of accusing public figures of being former secret services employees or collaborators not via statutory lustration procedures, but through rumours spread in the media and usually supported with stolen secret files in illegal possession of private persons or institutions.
34. Łoś and Zybertowicz, 2000, pp. 155–159; Milczanowski, 1997; compare http://www.rzecznikip.gov.pl.

on the direction of their work. The Commission relies on the information presented by the Directors of these services, examines their annual reports and offers recommendations or requests concerning the appointment of particular persons as Directors and Deputy Directors of the services. The Commission assesses draft budgets concerning the services and considers the report on the execution of this budget. The Commission also deliberates on cooperation between the services and the organs of the state administration and the prosecutor's office, as well as examining complaints concerning the activities of the services.[35] In 2003, the Commission contracted four experts, mostly former operatives or Directors of the services.

The Commission's first challenge came in December 1995 when the UOP, still under President Wałęsa's jurisdiction, made an allegation that the then Prime Minister Józef Oleksy, a former communist official, had been spying, first for the KGB and later for Russian Intelligence (from at least 1983 until 1995). The investigative powers of the Commission were very limited and the conclusions reached did not satisfy either side of the conflict. Another problem is that members of the Commission tend to have personal relationships with the objects of their oversight. Lucyna Pietrzyk, an MP, who was in the sub-commission investigating the Oleksy case, was employed by the ministry of the interior within which the UOP operated at the time.

Similar problems appeared in the following years. Konstanty Miodowicz, formerly the Director of the counterintelligence department of the UOP, has been a member of the Commission for the last two terms of the Sejm. He was publicly accused of being a so-called 'undercover functionary' (Barański, 1998). These accusations were never officially rejected as false. Miodowicz himself, in turn, publicly stated in 2000 that the sub-commission investigating the Oleksy case included secret collaborators of the former communist services. This allegation, like so many others in contemporary Poland, was never duly substantiated nor discarded as false. Cases like these make doubtful whether oversight is truly independent. Conflicts of interest seem to remain, and the political willingness of parliamentarians to scrutinise the services' activities remains an open question.

*Judiciary*

The use of eavesdropping methods is subject to approval of the General Prosecutor[36] and the District Court of Warsaw.

Under the statute of 6 April 1990 made by the Office of State Protection (UOP), there was, in theory, an independent judicial review of the UOP Director's decisions that on the grounds of national security certain information should be withheld from the investigation of the prosecutor's office. An opposition MP and member of the Sejm Commission for the Special Services, Zbigniew Wasserman,[37]

35. See the official website of the AW, available at: http://www.aw.gov.pl/en/.
36. In Poland this role is performed by the Minister of Justice.
37. Zbigniew Wasserman held the position of acting National Prosecutor (just one step below the General Prosecutor) in the cabinet of Jerzy Buzek.

has revealed that he can report more than a dozen cases of criminal investigations dealing with abuse of power by employees of the Office of State Protection (UOP) which could not be continued because Directors of the UOP refused to provide evidence demanded by the prosecutor's office. The refusal was justified for national security reasons. A reasonable procedure of verification of such refusals by the UOP existed in the UOP's statute of 6 April 1990.[38] Once in conflict with the prosecutor's office, the service's Director should provide relevant materials to the president of the Supreme Court. After examination of the materials, the president would make the final decision as to whether the material in question should or should not be provided to the prosecutor's office so that an investigation could proceed. However, the key point is that the UOP was actually capable of preventing this procedure from ever being applied. In one such case, the activities of the prosecutors were blocked by a decision of the then Prime Minister, Włodzimierz Cimoszeiwcz (Wasserman, 2002, pp. 16, 19).

## The State Captured?

The massive institutional shifts which have been underway since the end of communism have provided extremely fertile grounds for the proliferation of informal power networks in the Eastern and Central European countries. Legally unregulated lobbying, myriads of cases of conflict of interest, rampant corruption, limited efficiency of the police and ministry of justice are equally preconditions as well as results of the operation of such networks.

A prime example of the operation of these networks is the case of the FOZZ scandal (the Fund for Foreign Debt Servicing). A huge abuse of public funds was revealed in 1990, the materials were sent to court in 1993 but the case remained unsettled through the winter of 2004/2005 and is now likely to reach the expiration deadline.[39] When in 2001, a group of nineteen right-wing MPs put forward a proposal to the Sejm suggesting that the role of the secret services in the scandal be investigated, they were simply outvoted (Cieśla, 2003, p. 18). Only in the twelfth year since launching an investigation into this case has it become publicly acknowledged that key figures of the FOZZ operations were closely connected with the communist military foreign intelligence (Gargas, 2003, and Ordyński, 2003). Another symptomatic case is the illegal international arms trade pursued by the Military Information Services in the mid-1990s, which was another big scandal revealed in 2002 (Marszałek, 2002, 2003a, b). This case was investigated by the Sejm Commission for Secret Services which produced a report confirming the press accounts and accused the WSI of many irregularities. The Commission discovered that the networks used in this illegal trade had originated in the 1980s (Raport speckomisji, 2003; compare JRZ and JZ, 2003).

38. This procedure is also included in the new laws on the civilian and military services.
39. See for example Cieśla, 2003; Gargas, 1997; Kasprów, 1998; Łoś and Zybertowicz, 2000, pp. 165–179.

Circumstantial evidence suggests that the most powerful of the informal power networks are still based on resources generated by the institutions of the communist police state before 1989. The actors involved in those institutions inherited, successfully redefined, and now manage a much higher amount of capital than is the norm in Polish society. In similar contexts, experts on East European development from the World Bank discuss the 'capture of the state' phenomenon (see, for example, Hellman *et al.* 2000; Hellman and Schankerman, 2000). State capture is usually defined as the efforts of a small number of firms (or such groups as the military or corrupt politicians) to shape the rules of the game to their advantage through the illicit, non-transparent provision of private gains to public officials. Examples of such behaviour include the private purchase of legislative votes, executive decrees, court decisions and illegal party funding. However, unlike the World Bank's experts, the author claims that in the post-Communist countries the capture is mostly pursued by the business-security complex not by firms.

The undercover community constitutes a barely tangible nexus of interests, resentments and loyalties. This nexus has strongly contributed to the spread of clientelism in Poland.[40] Among clients of the security complex one should include members of the political elite (for example, Miller, 1998, p. 105), but also to some business groups and segments of organised crime (Biernacki, 2002, pp. 9–10).

All this, in turn, has brought about the phenomenon described as the institutionalisation of non-accountability.[41] It was possible because, as observed by Maria Łoś, 'the security complex represented knowledge and power modality that conditioned and penetrated all other social power forms' (Łoś, 2003; compare Biernacki, 2002). Delays in the preparation and then in the passage through parliament of the statute on the Military Information Services (as late as July 2003) – in a version that provided the WSI with too much freedom of action – is seen as an example of the influence of the security complex (Macierewicz, 2002).[42] Another well known example of the strength of the security complex is the way the open conflict was resolved between Lech Kaczyński, the Minister of Justice in Jerzy Buzek's cabinet in 2001, and the then chief of the UOP, Colonel Zbigniew Nowek. The clash was over whether the Minister, in his capacity as the general prosecutor, should order the detention of a deputy chief of the Katowice branch of the UOP who was a suspect in a financial scandal. The UOP functionary was released on the personal recommendation of the Prime Minister, and the Minister of Justice was instead dismissed (Kaczyński, 2001).

One could even venture to support another strong proposition of Maria Łoś, namely that:

---

40. As a general label, 'clientelism' describes the social organisation of both communist and post-communist countries. It can be defined as 'a network of social relations where personal loyalty to the patron prevails against the modern alternatives of market relations, democratic decision making, and professionalism in public bureaucracies' (Sajo, 1998, p. 38).
41. Hausner and Marody, 2001; compare Staniszkis, 1999.
42. See also various press accounts gathered at an informal webpage of former officers of the dissolved UOP, especially: http://www.uop12lat.republika.pl.

> some of the post-communist countries seem to have reached a point where illegal, parasitic webs have permeated agencies important to the functioning of the state to such an extent that a battle against them threatens the integrity of the state itself (Łoś, 2003).

It seems that this may partly explain the quasi-reform of the services mentioned at the beginning of this chapter.

At the same time, parts of the security complex have managed to present themselves as useful allies to the NATO authorities, shifting from one master (Moscow) to another (Washington). Whenever criticised, they invoke the external legitimisation of their existence and activities in order to prevent any thorough reform and supervision (Maloj, 1998). As noted by Williams, in Central and Eastern Europe:

> the pursuit of NATO membership has been substituted for serious discussion of what it means to feel safe or unsafe in a multi-polar, globalised Europe. This is alarming, since effective control of security intelligence presupposes that it should not fall to the services to decide what or whom to consider a threat; these are political issues requiring open debate and public awareness (Williams and Deletant, 2001, p. 20).

Therefore, it is not clear whether the services could become an instrument in the hands of the state in the fight against corruption and clientelism. The services first of all appear to be an instrument of an informal system which perpetuates the influence of political, party-centred, client-patron structures of control over the distribution of resources (Sajo, 1998, p. 39).

## Conclusion

The Polish secret services have neither been used for brutal wars abroad nor for repression at home, but are in effect a kind of lever for the pursuit of party politics and informal power networks that have nearly managed to capture the Polish state.

One could hardly say that the move from a closed and repressive apparatus towards a democratically accountable government service is complete in Poland. The services (not to mention the security complex in general) are not guardians of the public good, of the public resources, or the rule of law; they have become active agents in murky struggles over the distribution of the resources.

Poland does not have an intelligence policy that is truly in the interests of society. It seems that at present expunging inappropriate practices is beyond the power of any institution in Poland.

Instead of a system of good governance there is a system of institutionalised non-accountability, that is a soft state (in the classical sense of Gunnar Myrdal; compare Hausner and Marody, 2000). Myrdal, a 1974 Nobel Prize winner in Economics, initially coined the notion of the ‘soft state’ to explain the situation of countries which cannot embark on the path of self-sustaining economic growth. Soft states are characterised by rampant corruption, low levels of tax compliance

and enforcement underwritten by the absence of a work ethic both among public officials and in larger society, as well as the atrophy of all political will to correct these distortions. In soft states, governments require extraordinarily little of their citizens (Myrdal, 1968). Under the conditions of a soft state, the secret services usually present themselves as the hard core of the very state, which their activities often help to 'soften'.

Obviously, the security complex does not rule the country; far from it. The complex is not capable of performing such a 'positive' command. The impact of the undercover community is mostly of a negative nature. It infects democracy with non-transparent modes of operation (proffering unnecessary secrecy): makes exceptions a 'regime'; abuses the idea of 'public interest' in favour of partisan politics; undermines quality state institutions by imbuing the administration with the conviction that the officially declared procedures (indeed, the very idea of the rule of law) are to be paid only lip service, because what actually matters is the game of power (including resort to 'compromising materials'). The operations of the security complex prevent the emergence of cohesive political forces focused on fighting corruption and enforcing the rule of law. The complex provides the hard core of a parasitical system. This core is impenetrable due to its secretive nature. This makes it extremely difficult to eliminate the pathological phenomena from the social tissue.

Nearly two decades since the beginning of the transformation, the balance between the benefits and costs of personnel continuity is far from settled. It is not clear who has the upper hand. Are the services in the hands of democratic leaders, or are formally democratic leaders in the hands of the services? Most probably the game over the shape of Polish democracy is still unresolved (Zybertowicz, 2005). Will it become a fully fledged democracy underpinned by a robust civic society, or will it remain a shallow, formalistic system of power, regulated only from above, and by and large, limited to voting rituals?

One can also see a pendulum movement. When anti-communist political parties win elections and get into the government, they try to cut ties between the former communist era and the present-day intelligence services, even going so far as to abolish those services that appear hard to reform (for example the WSI). The pendulum then swings to the other extreme when post-communist political parties take over power in government and try to undo the reforms of their predecessor.

One could hardly conclude on a positive note. The vital point is not that the oversight system is obviously underdeveloped, nor the fact that the political scene has not yet sufficiently matured. The point is that both these factors reinforce each other. The process of maturation of Polish democracy must continue much longer before the strength of informal power networks inherited from the old system can be diluted.

Chapter 5

# Reforming the Intelligence Services in Bulgaria: The Experience of 1989–2005

*Nikolai Bozhilov*

**Introduction**

The post-Cold War years have been crucial for the Bulgarian intelligence community. New political realities have brought about a profound psychological transformation in intelligence thinking. This in turn has led directly to a complete revision of the professional perceptions of new allies, new enemies, new threats, and new priorities. For the moment, it is sufficient to say that this revision process is not yet complete. However, the protracted political struggles and constant attempts by political parties to gain control during the long transition period to democracy, as well as a market-based economy, have afflicted intelligence professionals with 'transition fatigue'. The notorious KGB-like image from communist times has been the source of considerable mistrust among the general public and has undermined the efforts of the intelligence agencies to deal with vital problems of national security.

Nevertheless, Bulgarian intelligence played an important part in the 1999 Kosovo crisis, siding with NATO and providing first-class support. An irreversible process of change and reformation began. Just how efficient this process will be remains to be seen. Its effectiveness will, to a large extent, depend on the political will of the party political establishment to rebuild the intelligence infrastructure in accordance with the threat assessment strategies of both NATO and the EU. Membership in both of these organisations does, of course, feature high on Bulgaria's strategic foreign policy agenda.

Despite some positive results coming from the maturing democratic society in Bulgaria, the 'intelligence community' is lagging behind. The existing national intelligence system is not sufficiently used and managed as a national resource. There is a clear need for effective oversight and control, the purpose of which would be to regulate inter-agency arrangements and implement the concept of an intelligence community. Cronyism, competing interests, rivalry, and protection of 'turf' are still part of the daily life of the intelligence agencies. Evidently, strong

political involvement is necessary with clear guidelines of accountability for all existing powers.

The 9/11 attacks against America both fragmented and activated the Bulgarian intelligence community, resulting in it being split into two major groups. Whilst one group tried to survive by means of political concessions, the other group was professionally motivated to use existing resources and to address security threats. The priority is now placed on the adjustment to the post-9/11 environment and on involvement in efforts to combat drug trafficking, the proliferation of WMDs, and international terrorism. Growing concern about transnational threats is leading to increasingly close cooperation between intelligence and law enforcement agencies as well as to the organisational changes in the intelligence community being considered. For ordinary intelligence officers, recent years have been marred more by political scandal and stagnant bureaucracy than reform. For the intelligence leadership it has been a balancing act between political survival and resource appropriation in order to respond to national security threats.

This chapter aims to explain the process that led to the present situation in Bulgaria. This is achieved firstly, by presenting a review of the historical background, which is necessary in order to gain a better understanding of certain Bulgarian perceptions, practices and prejudices; and secondly, by reviewing issues concerning accountability and oversight, and finally, by considering prospects and potential courses of action. Furthermore, this chapter focuses on and is limited to the activities of the main intelligence organisations – that is, the National Intelligence Service (NIS), the Defence Information Service (DIS) and the National Security Service (NSS).

## Historical Background

At the end of the Cold War, the Bulgarian intelligence model, a replica of the Soviet intelligence model, included a state security apparatus (a division of the ministry of the interior) comprising six directorates. These directorates were:

- Foreign intelligence;
- Domestic counterintelligence;
- Military counterintelligence;
- Technical intelligence;
- VIP protection; and,
- Political counterintelligence.

The post-communist history of the Bulgarian intelligence services can be divided into three periods. The first lasted from 1989–1997, when the Bulgarian political establishment was dominated by the structures of the former communist party, which was later renamed as the Bulgarian Socialist Party. The only exception was the right-wing government of Philip Dimitrov (1992–1993). The second period

started in 1997, when the Union of Democratic Forces with Ivan Kostov as Prime Minister took over the government. This period was to end with the tragic events of 9/11. The third period is the post 9/11 transformation, in which the war against terror has drastically changed the risk perception, even among the most conservative elements of the intelligence community.

It was during the period between 10 November 1989 and 10 April 1997 that the first significant changes took place. The Soviet triumvirate model (communist party – ministry of the interior – ministry of defence) was transformed into a bi-polar model of divided executive authority (President – Prime Minister). This led to the almost inevitable duplication of activities which resulted in a marked and rather dramatic loss of professional effectiveness. What followed was an orchestrated reorganisation, 'depoliticisation', and renaming campaign of the various services. This was designed to 'modernise and restructure' the intelligence community, although this was never publicly admitted. However, this was to become a protracted game of smoke and mirrors, for in truth little really changed. The power remained where it had always been – in the hands of a small, high-ranking ex-communist intelligence and security elite that pulled the strings both from within and outside the services.

Foreign intelligence (the National Intelligence Service) and VIP protection (the National Protection Service) were subordinated to the President – both of them being forced to penetrate domestic structures, an effort which was intended to compensate for the lack of presidential power over domestic issues. The ministry of the interior retained control over counterintelligence, which was then renamed the National Service for Defence of the Constitution and later the National Security Service, while part of the operations of the political counterintelligence were transferred to the newly created Central Bureau for Fighting Organised Crime. These transformations not only led to the disruption of Communist Party unity in the intelligence services, but also to a lack of coordination and efficient tasking. Corporate and vested interests began to cripple operations. During this period, operational work was severely disrupted by strong political interference. The services themselves were used as instruments to cater for the economic interests of the political establishment, providing information on lucrative privatisation deals, take-over assessments, strategic economic analysis, deception and information operations against opponents. This political interference damaged the effectiveness of some of the most straightforward and routine operations.

During the time that Prime Minister Ivan Kostov was in charge of the government (that is, from 1997 to 2001), Bulgaria became publicly orientated towards the West and NATO membership became a prime goal, backed by political consensus. The Kosovo Crisis was a milestone for Bulgarian foreign policy in general and for the intelligence community in particular. There was much practical cooperation with the major NATO Allies and an unusual amount of information and intelligence sharing. It was 'unusual' because one has to consider this in the light of the recent past, in that old habits and practices were still fresh in some peoples' minds. There had been an almost automatic reluctance to admit, share or even, in some cases, to discuss anything of real value. To do so would diminish one's own position. After all, there were no formal contracts in place and

nothing actually had to be done cooperatively. The intelligence world is nothing if not practical and pragmatic. A sense of realism had to penetrate into the whole of the Bulgarian intelligence community. During this first effective post-communist government, military intelligence was separated from the General Staff and renamed the Defence Information Service, and more significantly it was directly subordinated to the Minister of Defence. The General Staff of the Bulgarian armed forces retained only the tactical army intelligence. A new Financial Intelligence Bureau Directorate was established as a structure of the Ministry of Finance, and a Security Council, which was subordinated to the Prime Minister, was created with the aim of coordinating the efforts of the whole of the intelligence community.

The second major turning point, or test, came on the fateful day of 9/11. Contacts with western intelligence services were intensified, both in terms of increased frequency and in terms of subject matter. At the same time, some very basic work ethics and organisational structures were revisited. The period after 9/11 brought personnel changes in the leadership of two intelligence agencies – the National Security Service and the Defence Information Service. These changes were not a result of the increased post-9/11 requirements for efficient leadership, but rather of a political reshuffling after the governmental change and presidential elections in 2001, as well as the natural process of retired high-ranking officers being replaced.

## Democratic Accountability and Intelligence Oversight in Bulgaria

Executive oversight of the intelligence community in Bulgaria is split between the President and the Prime Minister. On the one hand, the National Intelligence Service (NIS) and the National Protection Service (NPS) are subordinated to the President. The President also chairs the National Security Advisory Council, the status of which is defined by national law. On the other hand, the Security Council at the Council of Ministers, the National Security Service (NSS) and the Central Bureau for Fighting Organised Crime (CBFOC) within the Ministry of the Interior, as well as the Defence Information Service (DIS), the Defence Counterintelligence and the Military Police within the Ministry of Defence, are all subordinated to the Prime Minister.

As mentioned earlier, this chapter is, however, limited to the activities of the main intelligence organisations – that is, the National Intelligence Service (NIS), the Defence Information Service (DIS) and the National Security Service (NSS).

### *Legal Framework*

The basic legal framework consists of the Constitution, the National Security Concept, the Law on Defence and the Armed Forces (covering the DIS), the Military Doctrine, the Law of the Ministry of the Interior (covering the NSS) and the new Classified Information Act. The intelligence agencies are governed in their work by secret statutory rules and regulations, which are approved by the

Bulgarian President and the Prime Minister. Despite the preparation of several drafts for an Intelligence Act that was to regulate Bulgarian foreign intelligence service (NIS), there has not been any progress so far nor is any expected in the near future due to a lack of political will.

In compliance with the Constitution of the Republic of Bulgaria, the President, the Parliament (National Assembly) and the Council of Ministers have responsibilities to the national security service.

The President chairs the National Security Advisory Council (NSAC). The NSAC includes the President himself, the Prime Minister, the Minister of Foreign Affairs, the Minister of Defence, the Minister of the Interior, the parliamentary leaders of the political parties represented in parliament and the heads of the intelligence and security services.

The National Assembly is responsible for enacting the legal framework of the national security system. Through its Permanent Commission for Foreign Policy, Defence and Security it controls the executive power and the special security organs as far as compliance with the law and effectiveness of actions are concerned as well as the efficient use of resources. It is also in charge of assessing political risks.

At this point, some further explanation of the Classified Information Act – the most recent controversial legislative act related to intelligence vetting activities – is necessary. The Act was passed by parliament on 24 April 2002. The law regulates what constitutes classified information and who should have access to it. However, the law also deals with the former files of the communist-era State Security Secret Service. According to the Bulgarian Government, the NATO reaction to the law has been 'more than good – very positive indeed' (Passi, 2002). The law is extremely well drafted; yet what remains to be done is to apply it. The Act and subsequent amendments have had little, if any, impact on transparency. The Act provides that the state services, including the ministries of the interior and defence should turn over the declassified records to the State Records Office (SRO), but this has not yet been done. Various institutions still maintain this information and strictly limit public access to it, despite the fact that it has been formally declassified. The State Commission on Information Security (SCIS) proved to be unable to impose any penalties for the violation of the Classified Information Protection Act (CIPA). The Council of Ministers was the only institution that turned over its declassified documentation to SRO following direct instructions from Prime Minister Simeon Saxe-Coburg-Gotha.

In January 2005, the Council of Ministers adopted new amendments to the CIPA that provoked broad public debate. The main reason was the abolition of control by the SCIS over the destruction of declassified information whose term of classification had expired. On the one hand, this virtually allows the ministries of interior and defence and the National Intelligence Service to destroy *unchecked* such information a year after it has been declassified. The draft did not make provisions for the respective institution to publicly announce the declassification of any records. On the other hand, under the new provisions, the possibility of legally challenging before the Supreme Administrative Court the destruction of declassified information authorised by the SCIS, was removed. Declassified

information that is of historic, practical or referential importance, should be turned over to the SRO. Moreover, the importance of the information should be evaluated by the institutional commission itself, with no representative of the SRO taking part. The amendments will also allow the SCIS to manage the archive of the commission that was established under the Law on Access to the Archives of the Former State Security and Former Intelligence Directorate at the General Staff (the so-called Andreev Commission). The SCIS will use it to certify the affiliation of persons to the Communist-era security apparatus and will declassify those documents whose term of classification has expired. Access to the archive has not been permitted since 2002, when the current CIPA was adopted. The draft is filed at the National Assembly, but has not yet been adopted.

No institutional changes have been made in Bulgaria's intelligence community either. A vision for the country's special services is provided in the Bulgarian Socialist Party's (BSP) Governance Programme, which advocates structural and functional centralisation of the special services, with the Security Council at the Council of Ministers emerging as the principal body for coordination and control. Once elected, the BSP envisaged the creation of three intelligence agencies:

- The Security Agency (comprising what is now the National Security Service at the Ministry of Interior and the Security Service, Military Police and Military Counterintelligence at the Ministry of Defence), which would be subdivided into four directorates (Internal Security, Military Security, Counterintelligence and Operational & Technical Intelligence);
- The Intelligence Agency (successor to the current National Intelligence Service, which is subordinated to the President); and,
- The Protection Agency (similar to the National Protection Service, which is also subordinated to the President at present).

However, real changes will be difficult to implement due to contradicting visions among the coalition partners in the new Bulgarian Government which was formed in August 2005. In many ways, this law even surpasses NATO standards because it incorporates the experience of countries such as NATO's new members Poland, Hungary and the Czech Republic, which have faced problems similar to those being experienced by Bulgaria. However, the reality is not as straightforward as it seems. Under the provisions of the new law it will be impossible for researchers to establish a clear picture of the state security organisations' work because it gives the government authorities the right to reclassify documents that would otherwise be open to the public. The new law provides for four different levels of secrecy, ranging from 'top secret' to 'internal use only'. The 'top secret' documents are barred from publication for 30 years. The main flaw of this law is the lack of any effective control mechanism. The law provides for the formation of a State Commission on Classified Information, whose five members are to be appointed by the Prime Minister. The opposition party, Union of Democratic Forces *(Sajoz na Dcmoknatichnite Sili*, SDS), demanded that at least two of the five members be

nominated by the parliament to ensure a minimum of public control over the commission. Some experts argued that the authors of the new law should have advisors who ensure not only that the archives of the State Security remain out of reach of the society, but also that the future actions of the authorities are carried out in a satisfactory manner. According to one of the experts, '[t]he sad truth is that whoever comes to power will decide that the law is good for the government and bad for the opposition and hence will decide to leave it as it is' (Dimitrov, 2002, p. 7).

*Parliamentary Oversight*

According to the Constitution, the parliament is responsible for the approval of the governments' budget, which includes the budget for defence and security. The oversight of the intelligence agencies falls to the Parliamentary Commission for Foreign Policy, Defence and Security – CFPDS (*Komisia po vanshna politika, otbrana i sigurnost*). In practice, parliamentary oversight is almost nullified by the lack of proper parliamentary organisation, staff and expertise. Out of 28 members of the CFPDS, currently only one member – the former chief of foreign intelligence – has the necessary expertise. The Commission is entitled to ask for the presence of the Directors of the intelligence agencies, if required. In general, parliamentarians have been reluctant to share responsibility with the government or to scrutinise the intelligence agencies, except in cases of public scandal or emergency. Furthermore, parliamentary oversight is complicated by the lack of a comprehensive law for the foreign intelligence service (NIS).

*Executive Branch Oversight*

The civilian oversight of the Defence Information Service (DIS) and the National Security Service (NSS) is provided through the Minister of Defence and the Minister of the Interior respectively, who report to the Prime Minister and the Council of Ministers. Both Ministers participate in the Security Council of the Council of Ministers. The Security Council is comprised of the Prime Minister, the Minister of Foreign Affairs, the Minister of Defence, the Minister of the Interior, their deputies, the chief of general staff of the Bulgarian armed forces and the chiefs of the intelligence and counterintelligence organs. The President personally, or through his representatives, can always participate in the work of the Council and can request information from it at any time.

As per Article 55 of the National Security Concept, the Security Council has the following responsibilities:

- It summarises, analyses and draws conclusions from all current information about risks to national security and makes a professional assessment of, and prognosis for, the dynamics of the threats;
- It plans concrete measures for the neutralisation of threats and proposes solutions in times of crisis;

- It coordinates the plans of the special organs for the acquisition of information resources; and,
- It develops an annual report on national security which it then puts before the Council of Ministers. The President, the Chairman of the National Assembly, and the Prime Minister can request information from the Security Council.

Curiously, the Security Council is supported by a small number of 'experts' who are not on its payroll but who occupy positions in the Council of Ministers. This practice needs to be re-examined for at least two reasons. Firstly, the Council does not provide independent intelligence assessments; and secondly, it has no practical coordinating functions. One of the possibilities is to upgrade the existing Security Council to that of a statutory organisation or to follow another possibility – the practice in the Anglo-Saxon world where a Joint Intelligence Committee (UK) or Intelligence Advisory Board (US) is appointed to coordinate intelligence activities. It is common practice in these bodies to hear evidence from a range of experts, instead of solely from agency officials.

Another major problem is the lack of a statutory mandate for the Directors of the intelligence agencies. They can be appointed and dismissed at any time during a political reshuffling. The old argument of whether the national intelligence services are a party political matter or whether they are above such squabbles is still unresolved. This situation does not mobilise or motivate heads to implement institutional changes and modernise their services. There have been intensive discussions over the last few months among all powers in Bulgaria about correcting this situation as soon as possible.

*Judicial Oversight*

Bulgarian intelligence agencies operate under a legal framework. According to the Act covering the use of special technical means, the intelligence agencies are not legally allowed to covertly collect data and evidence against a citizen without receiving permission to do so from the judiciary.

## The Bulgarian Intelligence System – the Post-Cold War Changes

Taking into account the contemporary methodology to assess intelligence capabilities on the basis of the three-tier approach: people, process and technology, an independent assessment is offered of what has changed in the work of the intelligence organisations during the last 15 years and especially after 1997, when the real changes began.

*People*

During the Cold War, recruitment and career management were entirely controlled by communist party interests and through the subordination of the intelligence

services to the totalitarian regime doctrines. It was common practice for intelligence officers to be recruited from high-ranking party and intelligence officials' families. This practice continued for some time during the transition period but has gradually decreased over time because of the diminishing public influence of the services, political uncertainty, low pay and lack of career prospects. The process of recruitment was additionally hampered by continuous political screening and mass purges every time the ruling political party formed a new government.

Little change can be seen in the recruitment process during the last decade; old and traditional methods still prevail in the form of recruits coming from specialised classes in military schools and on the basis of personal recommendations from serving officers. A few talent scouts operate in universities, defence colleges and the army. Recruitment and training are still largely based on the old Warsaw Pact thinking concerning threats to security. The efficiency of the recruitment process is hampered by very serious constraints, linked to the following problems.

Because of the 'brain drain' from the country and a rapidly growing private sector and especially given the lack of any open public recruitment, it is becoming increasingly difficult to find bright, intelligent young people who are ready to commit themselves to the intelligence world. The intelligence profession is no longer considered attractive, prestigious or well paid – facts which coincide to a great extent with the negative public opinion about intelligence services. There is a lack of legislative guarantees for the profession. Clear, fair and motivating career prospects are lacking for ambitious young people. At present, available recruitment sources remain limited and for a while, the restructuring of military education brought about a dramatic fall in recruitment standards, particularly in defence intelligence.

On paper, the criteria for recruiting people into the services have been raised to unnecessarily and unrealistically high standards. Vetting and probation procedures have in practice changed very little. Each service has its own procedures for recruitment and probation. The heads of the service department usually set out the requirements for new recruits one year in advance. After a pre-selection of suitable candidates, the screening period may take up to 12 months, during which time the selected candidates may undergo several interviews with the special recruitment commission or its representatives. Once again, due to the number of vacancies, the probation period is sometimes all too easily passed.

Another problem area is the education and training of new recruits. After joining an intelligence organisation some are sent to internal education and training facilities, where they spend between 6 and 24 months, depending on their previous experience and educational background. The problems of the modern intelligence education and training arise from the fact that teaching personnel are either from the Cold War era or lack international experience and training exchange with foreign intelligence agencies. As a result, there is limited teaching of modern intelligence techniques. Very often no distinction is made between security and defence – thus intelligence training is adapted to defence challenges rather than security challenges. In addition, new intelligence priorities require experts in the

new security challenges such as anti-terrorism, organised crime, Islamic extremism, non-proliferation of WMDs, cyber-warfare and so on – subjects that are difficult to teach without practical experience.

The lack of motivation and career development programmes seems to be the greatest constraint on identifying qualified recruits. One of the strongest sources of motivation is not only money but good career prospects as well. Unfortunately this is often forgotten. Therefore, there is need for coherent personnel policies, based on clear criteria which will make a substantial improvement in the recruitment and advancement of intelligence officers, amongst whom the majority desire to be given a position on individual merit, not on patronage, cronyism or nepotism. In contrast to the military, very few intelligence experts are sent to training courses in the West, but those that are – like the military – are then excluded from advancement in their career. The repercussions of this are obvious. Those who do go find themselves being professionally cold-shouldered on returning to Bulgaria and rapidly become very disillusioned. This is not always easy to hide and is frequently witnessed by others. The effect is contagious. There is then a marked reluctance among other potential travellers to go to western colleges and institutions due to the negative effects, both professional and personal, that this has on one's career. A vital question is therefore, how to break this cycle?

*Processes*

The mission of the intelligence services has changed dramatically in the post-Cold War era. Intelligence analysts are challenged as never before to be creative and proactive in meeting intelligence needs. Lengthy analytical papers largely focused on the Warsaw Pact perception of the NATO threat that were the norm 15 years ago have to give way to a combination of briefings and short, but insightful, intelligence products covering a broad range of national, regional and global issues.

Now more than ever, new products must be tailored to the individual intelligence consumer's concerns and the analysts have to put the highest premium on knowing what their consumers need. The revolution in information technologies has improved access to a whole range of sources and has increased the ability to deliver intelligence quickly. Yet it has also made intelligence work more challenging as analysts are bombarded with information of varying quality, relevance and depth. To meet the challenge of political change and technological advances and to take advantage of the opportunities they present, the Bulgarian intelligence agencies are in the process of re-examining their core analytic 'tradecraft' skills and updating them to reflect how they do their business.

The pursuit of expertise in analytical tradecraft is a central element of this action plan. The tradecraft enables analysts to provide 'added value' to consumers of intelligence by ensuring dedication to objectivity, which enhances credibility with consumers dealing with complex and sensitive policy issues. The timely delivery of intelligence products to the policy makers is paramount. Moreover, the feedback and tasking from them to further drive the collection of the basic

intelligence for analysis production is a two-way process that needs an educated intelligence culture.

Traditionally, since totalitarian times, Bulgarian intelligence has been quite efficient in the collection and processing of human intelligence (HUMINT). Being the staunchest ally of the Soviet Union during the Cold War, Bulgarian intelligence agencies possess an intimate knowledge of the Soviet-era mentality and the Soviet-style operations that continue to prevail in today's Russian intelligence and in certain other former republics of the Soviet Union. Another area of competence is the Near and Middle East, where work with some Arab special services has been done in the past. Furthermore, the inside knowledge of the relatively insecure and troublesome Balkans and other countries in Southeast Europe do, of course, represent a particular asset in present and future intelligence-sharing with friendly services from NATO, the EU and others.

The *modus operandi* of the Bulgarian intelligence system is gradually starting to change. Perhaps the most significant change comes from the new political realities that have brought to the fore new allies and new enemies. The Cold War priorities have been largely replaced by the challenging priorities of combating international terrorism, the proliferation of WMDs, drug trafficking, illicit arms trading, and other serious organised crime. This seems to be a daunting task for the senior officers in the intelligence agencies, whose entire careers have been dedicated to researching and monitoring the defence capabilities of the NATO countries.

Recent years have brought a substantial increase in the use of all-source information for intelligence products. It has been recognised that analysis needs a fresh approach and that more human resources are directed to this requirement. A much greater proportion of information has been obtained without the use of human agents or sophisticated collection platforms. At the same time requirements for translation, systematic analysis and dissemination have further increased.

In their restructuring, the intelligence organisations face very serious challenges. Methodology from the Cold War era is part of the daily work. Corruption is a serious problem in some agencies. Senior officers outnumber junior officers. Indeed, the whole career 'triangle' is wrong. Due to the lack of a career management system and scant financial resources, motivation is often missing. There is an urgent requirement for a new system of documentation of the intelligence personnel files. Operational work needs to be tailored towards better information security and diminishing corporate and vested interest penetration. It is important to have a modern legal basis for strictly need-to-know information access. The psychological barriers to public-private partnership and collaboration with NGOs and academia are very high indeed. There is not enough debate and dialogue with outside experts about intelligence and the multitude of threats the modern world faces today. Unlike the military, contacts with western intelligence organisations have still not resulted in the training of intelligence personnel to work in joint intelligence quarters or in joint intelligence operations. Another important factor in the training of qualified intelligence personnel is the ability of officers to rotate between the different services in order to gain additional experience.

A further consideration needs to be explained: communication and secrecy in the intelligence work. Communication with society as a whole has always been a problem for the Bulgarian intelligence agencies. This problem has been brought about not only because of the secretive nature of the work but also due to the reluctance of the leadership to allow the public to get closer and to make its work more accountable. The concept of winning 'hearts and minds' of society even with limited and balanced reporting is an essential tool in modern communications. Unfortunately this has never been part of the intelligence chief's toolbox. Nevertheless, the media have always shown a strong interest in intelligence matters. At the same time, the media have been somewhat irresponsible in writing about intelligence services. A typical example will serve to illustrate my point. At the beginning of 2002, a report appeared in one of the Bulgarian newspapers about 'information' of a secret al-Qaeda meeting in Sofia. The administrative burden that fell on the intelligence services was to explain that the information was groundless and was only a simple attempt by the journalist in question to become noticed. Such cases make intelligence agencies very cautious in their contacts with the media.

Secrecy is a vital element in the work of the intelligence agencies for a number of obvious reasons. Advance knowledge of an enemy's plan may open up the possibility for a successful operation. Another reason may stem from doubts over the collector's legality and propriety. The most important reason is probably the collector's vulnerability to countermeasures and source protection. In peacetime, however, it is sometimes advantageous to create a public impression of being well informed as this has normally a deterrent and preventive effect. It is especially valuable in achieving foreign policy objectives, but can play strongly against you when it is used in a clumsy and inappropriate way.

During the presidential elections in 2001 – the incumbent President Stoyanov, who had a high degree of electoral support and could have easily won in the presidential contest – took the liberty during a televised debate, of showing the public a secret report by one of the intelligence agencies which alleged that the other candidate was involved in corruption and connected with certain economic vested interests. This act was interpreted by the general public as a serious abuse of presidential authority. As a consequence of this and other mistakes, the most popular President in Bulgaria's post-communist history lost the elections. On other occasions, the short briefs and Q&A exchanges by the Director of the National Intelligence Service with media have had a very positive effect. That is why secrecy should not be a reason to keep society uninformed of the trends and general achievements of the services.

Finally, it is necessary to emphasise the international cooperation of the intelligence agencies, which is considered the strongest driver of change. Intelligence has its enemies but it also has its friends. The international system of intelligence cooperation is not new in principle, but is relatively new for the Bulgarian agencies in the post-Cold War period. Allies have always shared some intelligence in war and information exchanges have always been part of diplomacy. As mentioned previously, the intelligence sharing with NATO that began during the Kosovo crisis later evolved into one of the most important components of the

eventual future integration of Bulgaria into the Euro-Atlantic Alliance. The cooperation with USA, UK, Germany, and other NATO allies became part of the routine intelligence work and boosted the reformation process. This process also brought new knowledge about modern threats and the methods to counteract them efficiently. The cooperation was expected to become very intensive once Bulgaria was invited to join NATO. Integration and liaison will be powerful elements for the refashioning of the Bulgarian intelligence system in the years to come.

There have been however several problems in this process. The accession of Bulgaria to NATO posed a security risk as Russian penetration and vested interests in the government and the intelligence services could not be ruled out. Yet, there was no clear positive vetting programme that could satisfy NATO needs. These problems were surmountable as firstly, NATO information sharing is strictly on a need-to-know basis; secondly, for Bulgarian nationals who will receive the highest NATO security clearance, vetting was likely to be carried out by a major western counterintelligence service (Galleotti, 2002).

## Conclusion

Intelligence work in the post 9/11 era is an arduous task and its assessment requires a close look at management, process and technological developments. It also requires a determined long-sighted vision and a strong political will to bring Bulgarian intelligence agencies up to much-needed higher standards of professionalism than previously existed. This in turn requires a clear and objective analysis of the new trends and new threats. This process can only be achieved by a public-private partnership and constant dialogue between the intelligence providers and the intelligence consumers. Bulgaria faces a moment of opportunity here; it must be seized and embraced by serious politicians so that the whole of Bulgarian society will feel the benefit.

However, much more effort is needed to create an effective democratic oversight mechanism. This process has been practically frozen by all post-communist governments despite the bold political statements. Unfortunately, after 9/11 the imposed veil of secrecy allegedly based on the newly adopted Classified Information Act has often been used by the political and professional establishment to justify the absence of any progress on reforming special services.

*This page intentionally left blank*

Chapter 6

# The Aftermath of 1989 and the Reform of Intelligence: The Czechoslovakian Case

*Oldřich Černý*[1]

## Introduction

To understand why following the huge changes of 1989, the Czechs and Slovaks decided to choose different paths to build their intelligence community than the rest of the Warsaw Pact countries, one has to take into account the political climate that existed in communist Czechoslovakia. This chapter offers a subjective recollection of someone who personally witnessed the whole 'hit and miss' process during these changes rather than being an attempt at a detailed history of the developments after 1989.[2]

The tumultuous events of 1989 began in Prague with the police beating up protesters honouring the memory of Jan Palach, who in January 1969 immolated himself in protest against the Soviet occupation of the country. At the same time in Poland, the round-table discussions were already underway and the Hungarians were engaged in a free discussion of the 1956 uprising. By June 1989 the Poles had their first semi-free elections filling the upper house of their parliament, the Sejm, with anti-communists while Václav Havel was still serving his last prison sentence. By August 1989 the governments of Hungary and Poland issued their apologies for the part their countries played during the 1968 invasion, causing huge embarrassment to the Czechoslovakian communists who were just getting ready for the August 21 demonstration planned by the opposition by arresting the dissidents and putting them into preventive detention cells. By October 1989 Guyla Horn allowed the East Germans into Austria. At the same time, Václav Havel was in hospital fighting pneumonia. On October 28, commenting on a disappointingly

1. Special thanks to Karel Pacner, Kieran Williams and Chris Donnelly.

2. The article presents a personal account of the author's experiences as National Security Advisor to the President of Czechoslovakia (1990–1993) and, following the split of Czechoslovakia, as the first Director General of the Czech Foreign Intelligence Service (1993–1998). For academic analyses of Czech and Slovakian Intelligence Services, see, for example, Kieran Williams and Dennis Deletant, 2001.

low turnout at the National Day demonstration, he was in a very pessimistic mood and was talking about Czechoslovakia as it were a Castro-like island in a sea of democracy. Then on November 17, everything changed nearly overnight.

## Dismantling Communist Intelligence: 1989–1992

While certain evolutionary processes were proceeding in Poland and Hungary giving their secret services time to reflect on them, regroup, and prepare for a new era, the Czechoslovakian secret services (the First and the Second Directorates of the STB, which was the abbreviation for the communist secret police – *Státní Bezbečnost*) were, to the last minute, together with the army and people's militia, tools of the Communist Party of Czechoslovakia. They were strong, feared and unreformable, and their structure was a mystery.

The situation in the first half of December 1989 was absurd. There was the first democratic government, yet the STB people still reported for work busily shredding their files, conspiracy theories abounded, and the seat of the Minister of Interior was strangely vacant. Officially, there were two Deputy Prime Ministers and a Prime Minister responsible for the Ministry of Interior but on a day-to-day basis it was run by General Aloiz Lorenz who until 17 November was in charge of both the First and the Second Directorates. General Aloiz Lorenz played a prominent part in destroying the documents, for which he was later sentenced to three years in prison, a sentence that due to the break-up of Czechoslovakia was never served. The shredding of files continued more or less uninterrupted until mid-December. The communist secret police were thus given ample time to cover their tracks and provide protection to their secret collaborators, a service which, they thought, could prove useful in the uncertain times ahead. This strange situation changed only after Václav Havel was elected President on 30 December. One of his first acts as President was to name Richard Sacher, a prominent functionary of the Christian Democratic Party, as the Minister of Interior tasking him to dismantle the STB so that the new regime would finally get rid of the climate of suspicion and fear. Richard Sacher set out to fulfil his role nearly immediately after he was appointed. He had closed down all politically compromised sections of STB, namely the huge directorate for the fight against the so called inner-enemy; all the officers had to hand in their badges and weapons and were transferred from active duty to the reserves. Therefore, we can say that as of mid-February 1990 the STB, comprising some 17,000 personnel, no longer existed.

Richard Sacher insisted that the STB officers should be dealt with according to the existing laws. All those laws, including the Labour Code, were designed by the communists' lawyers. The result was that most of those STB officers who left in the first months after 17 November were given hefty financial bonuses for the years they spent in the service.

Some of the STB officers made an assessment of their situation, did not wait for the screening processes to start, and left the services of their own will. This is particularly true of the officers of the First Directorate (Foreign

Intelligence) who knew foreign languages and had good contacts abroad. These people were among the first on the starting line of the new capitalistic world. However, most of their ventures sooner or later crashed because despite all their comparative advantages they never really understood the rules of a market economy and relied on the favour-for-favour system.

Those who did not leave of their own free will were subjected to systematic vetting by the Citizens Committees established by the Civic Forum and its Slovak counterpart Public Against Violence. Paperwork for the screening commissions was done by so-called 'troikas' (one former STB officer fired after 1968, one member of the citizens committee, and one current employee of the Ministry of Interior).

The vetting procedures were long, many mistakes were committed, and agents of the STB infiltrated some of the commissions; but on the whole one can say that the Second Directorate of the STB had been dismantled methodically and lawfully, and an institution that had plagued the Czechs and Slovaks with nightmares was completely ended. There were fears that the fired officers of the STB would form underground organisations and conspire against the new regime, but those fears never materialised.

Somewhat different steps were taken in dismantling the First Directorate, that is, the Intelligence Service. This service also operated under the Ministry of Interior and at the end of 1989 employed both at home and abroad approximately 1,300 people working on KGB orders in 35 countries all over the world. In the first two or three months the atmosphere at the First Directorate Headquarters was chaotic. There were rumours that the new regime would nullify the benefits due to those who were about to retire (generous severance pay and a special bonus) and most of the officers over 55 asked for retirement before Christmas. The officers abroad were gradually cancelling their meetings with their agents. Some of the officers, particularly in Washington, New York, London, Tokyo and Brussels were approached by their CIA counterparts with offers of cooperation. Most of them reported it to Prague, but Prague remained silent. Just before Christmas all six Soviet advisors left for their holidays vowing to return after the Russian New Year, a promise that somehow was never fulfilled. Otherwise, little happened until the end of February 1990 when Přemysl Holan (a former First Directorate officer and one of the first to be purged after the 1968 Russian invasion) was appointed as acting Director of the service. Holan's first directive to the First Directorate's station chiefs abroad was: 'Stop all activities immediately'. At the same time he ordered an audit of all financial resources, an act for which the author, as one of his successors, is still eternally grateful to him. At that time, Czechoslovakian intelligence had about 300 agents all over the world. Apart from the meetings that were already fixed a long time ahead and where the agents were told that the marriage was over, all of these people were left out in the cold practically over night. Recalling the 'illegals' was more complicated. Analyses of each individual case were made and the process took nearly two years to complete. There were some bizarre situations: one Czech intermediary was detected by the FBI in New York and rather complicated and awkward negotiations ensued. In summer 1990, the new Director of the service, Radovan Procházka, who spent fourteen years in

communist concentration camps, recalled all the embassy residents in Western capitals, installed a few declared representatives instead and recalled all operatives sent abroad without diplomatic cover. Despite all these steps, some continuity with the First Directorate still persisted until the division of the country at the end of 1992. The search for a new orientation was difficult and some old habits were dying very slowly.

## Building a New Intelligence Community

When it came to building the new institutions, there was a general consensus in society that the new Czechoslovakian intelligence community must be based on appropriate and relevant laws, must have parliamentary oversight, must be stripped of all executive powers (arrests, interrogation), must be tasked and coordinated by the government and should limit its activities to information-gathering and analysis with special emphasis on terrorism, extremism, and organised crime. Despite this universally shared consensus, the first version of the non-communist internal security service, *Úřad pro ochranu ústavy a demokracie* (the Office for the Protection of Constitution and Democracy – OPCD), was an unbelievable mess, convincing proof of the overall confusion in those days. The new democratic elite were 'babes in the woods' when it came to intelligence, so they turned for help to old professionals who eagerly volunteered for the top jobs. Those professionals were former STB officers fired after the 1968 invasion who spent the next twenty years in oblivion often working in manual jobs. The problem with some of these people was that they thought that in 1990 they could start working exactly where they had left off in 1968 or 1969, without taking note that nearly twenty years had passed and the world had changed a little bit.

The result was that for several months in 1990 the country had to cope with a big misunderstanding called the OPCD, which employed nearly 6,000 people and was structured along the lines of the old STB. Even though the new government clearly stated its foreign policy goals ('Back to Europe!'), a clearly stated security policy was painfully lacking. Two sections of the OPCD were focused on old enemies – the USA, Great Britain and Germany. Surveillance and technological (eavesdropping) sections were staffed by technicians from the old era who were kept busy by answering citizens' complaints regarding real or imaginary listening devices.

At that time, no new laws were even considered by the Czechoslovakian parliament, and oversight – mostly perfunctory and unqualified – rested solely with the Defence and Security Committee of the federal parliament. Privatisation of the economy, rehabilitation and restitution concerns were far more important than security issues. But the structure of the OPCD was too much to ignore. President Václav Havel therefore persuaded an old friend and former dissident, Jan Ruml, into taking a job at the Ministry of Interior with special responsibility for the OPCD. Jan Ruml purged the OPCD of most of the old veterans from the sixties and most of the remaining STB leftovers. With surveillance and technological departments becoming an integral part of the Ministry of Interior, the OPCD was

trimmed to roughly 1,000 people, mostly those who volunteered after 1989. It was a very strange bunch consisting of former dissident activists, 'grey zone' people, and band wagon jumpers, but a vast majority of them had one common denominator: no experience in security issues, tradecraft, or the ways an intelligence service should function in a democratic society. How did the country tackle this problem? The old STB schools were no longer in existence. Czechoslovakia simply asked its new western friends for help, which was given by the Americans, by the Germans, by the Dutch and, most of all by the British, who were extremely helpful in preparing and organising several very well structured courses both in Britain and Czechoslovakia. The graduates of those (and other) courses gradually assumed higher posts within the intelligence community hierarchy and some of them later became teachers and instructors themselves devising the curriculum for newcomers.

The new officers were taught by their mentors from the other side of the former Iron Curtain not only the basic elements of tradecraft, analysis, file keeping, etc., but also of the need for oversight and tasking and coordination by the government. The early 1990s in Czechoslovakia were marked by a great degree of passivity on the part of the politicians to address these important issues. Although most of these early politicians came from similar dissident or 'grey zone' backgrounds, after 1989 they chose different careers and went to different schools and the traumatic experience of forty years of the communist secret police was still strongly felt. This complete lack of governmental initiative to prepare and present the needed legislation led a group of parliamentarians to draft a law for the Federal Security Information Service (*Federální bezpečnostní a informační služba* – FBIS, the renamed OPCD) defining the mandate of the agency, the means that could be used to fulfil it, and the basic elements of control and oversight. The law detached the FBIS from the Federal Ministry of Interior, defined the mechanisms for appointing and removing its Director, and outlined the accountability of the Director to the parliament. This law, passed by the federal parliament in May 1991, was far from perfect (one major flaw: the FBIS was tasked by the government collectively which meant that no government Minister was responsible for the activities of the service) but at least laid down the groundwork on which to build. The foreign intelligence service remained a part of the Federal Ministry of Interior (a nice contradiction in terms remaining to this day), and no legislative steps in this regard were considered.

The first special parliamentary organ to oversee the FBIS was set up in January 1991, but it took several months before its members were cleared for access to classified information. Reluctance on the part of the government, followed by legislative haste resulting in mistakes, can be explained (but not justified) by two things. All of this was happening against the backdrop of the demise of the bipolar world when the traditional military threats were diminishing, and a host of new threats were ascending. These did not threaten the territorial sovereignty of the state but rather its very structure, the functioning of its institutions and the well-being of its citizens were grossly underestimated. Due to the opening of the borders, restitution and privatisation laws, huge masses of property were being exchanged without appropriate regulatory and control

measures in a country where the politicians bragged that the economists had overtaken the lawyers, which later proved a fatal mistake.

A lot of the Czechs and Slovaks were baffled by the new world unveiling before them. For example, in early 1991, when I served as President Havel's advisor in security matters, I was approached by two policemen from the town of Zlín near the border with Slovakia. They were worried about some Italian companies cropping up in their region doing everything but what they were registered for. The policemen suspected mafia activities and asked me to transmit their suspicions to the appropriate authorities. I handed over their data to a declared representative from SISMI (Italian Military Intelligence Service) whose response – a fortnight later – I will never forget: 'Don't worry, Mr Černý, we checked it very thoroughly and it is O.K., it is not mafia, it's only organised crime'. But how do you explain this subtle distinction to two policemen whose only knowledge of mafia comes from watching the Godfather movies?

Another important factor overshadowing everything else was the division of the country. Over the years of coexistence of Czechs and Slovaks, there had always been some nationalistic sentiments brewing on both sides. But after 1989, the lid was off and by the beginning of 1992 it was clear that the country was heading for separation into two independent states. The ratio for division of the property and other assets was determined according to the ratio of population, 10,000,000 Czechs, 5,000,000 Slovaks, therefore 2:1. The division of the military brought on some bizarre complications. Given the logistics of the Warsaw Pact, most of the combat troops were stationed on Czech territory while the schools, storage facilities and armaments factories were situated in Slovakia. Czechoslovak supersonic fighters operated from the Czech air bases but the only school for training the pilots was in the most eastern part of Slovakia and was staffed by Czech instructors. Good political will on both parts worked miracles and acceptable solutions were found.

But there was one problem that was giving nightmares to the Czech and Slovak spymasters: how do you split the archives of the secret services, which together with the army belonged to the most federalist institutions of them all? Finally, it was done on a 1:1 basis. This decision proved wise when later Vladimir Mečiar's Slovak Information Service became riddled with old STB cadres and showed its potential by kidnapping the President's son and other escapades. Although the relations between the Czech and Slovak services during Vladimír Mečiar's premiership were not exactly warm, knowing exactly what the other side had on its historical files prevented both sides from staging stupid antics against each other.

## The Czech Republic, 1993–2002

When the new republic officially came into existence on 1 January 1993, the spectrum of the Czech intelligence community did not change from the times of the Federation. There were still four services, two civilian and two military: (1) BIS (*Bezpečnostní informační služba* – Information Security Service), civilian

counter-intelligence, which was constituted by a law passed in undue haste in the last months of the Federation; (2) ÚSZI (*Úřad pro zahraniční styky a informace* – Office for Foreign Relations and Information), civilian foreign intelligence; (3) VOZ (*Vojenské obranné zpravodajství* – Military Defence Intelligence), military counter-intelligence and; (4) ZSGŠ (*Zpravodajská služba generálního štábu* – Intelligence Service of the General Staff), military intelligence.[3]

What changed was the perception of the intelligence community by the executive branch. To be a head of any Czech service in the first years of Václav Klaus' government was not easy. While the first two years after 1989 were devoted to dismantling the old communist secret police structures and building the new ones, the following years should have been devoted to gradual strengthening of the coordination and tasking, analytical and operational skills on one hand and further necessary legislative steps including oversight on the other hand. But Václav Klaus was an economics-focused pragmatic politician with an instinctive aversion to military and intelligence issues. Transformation of the economy of the country, which was slowed down by the division of Czechoslovakia, was foremost on his mind, and military and intelligence were considered 'Cinderellas' of the Czech establishment. Shortly after he became the Prime Minister he found out – most likely to his great dismay – that among other functions he did not expect to come with the premiership was the post of the Chairman of the Council for Coordination of the Intelligence Services. The British model of the Joint Intelligence Committee (JIC) inspired the creation of the Council, initiated in 1991, by a few representatives of the intelligence community craving more interaction between the intelligence community and the executive branch. The Council, consisting of the heads of the four services, the President's Advisor on security matters, the Prime Minister, Minister of Defence, Minister of Finance, Minister of Interior and Minister of Foreign Affairs, was a far cry from the JIC but at its best provided much needed dialogue between the intelligence community and the executive branch and as one veteran of those early days put it: '… at least they saw that there were no horns sticking out of our heads'.

Spurred on by journalists, Václav Klaus finally called for the first meeting of the Council for Coordination of the Intelligence Services in late March 1993. The atmosphere in the room was very nervous and Václav Klaus was late. When he finally came he sat down, looked over the room and said the famous words much quoted by the Czech press, particularly after 9/11: 'If I could I would dissolve you all, but I probably would not get away with it. So, what's on the agenda?' This can hardly be described as a promising start to a new relationship. But with the benefit of hindsight one can understand his reasoning. On the opposite side of the table were four people trying to scare him with uncontrollable waves of migration, instability in Russia, growing threats of international terrorism, nuclear smuggling and mafia-linked crimes. But the numbers just were not right. The results somehow did not justify the required expenditures, and the broader

3. For a concise overview of the Czech national intelligence community, see Henderson, 2002, pp. 197–200.

circumstances of the origin of the new Czech intelligence community completely eluded him.

Nevertheless, under pressure the government promised to present the parliament with a new law that would reflect the fact that there are four intelligence agencies in the Czech Republic (until such a law was passed the civilian foreign intelligence service and its military counterpart were – from a purist legal view – illegal organisations), define their mandates, means of control, oversight, tasking and the degree of political responsibility of the respective Ministers of the government. The work on the law was slowed down by the proposal made by the then Director of the BIS, Stanislav Devátý, who advocated the merger of civilian intelligence and counter-intelligence and, likewise, the merger of the remaining two military services into one. The idea was supported by Václav Klaus – who thought that when it came to the intelligence community, 'the less was beautiful and economical' – and opposed by the Minister of Interior, Jan Ruml, and the Minister of Foreign Affairs, Josef Zeleniec, who pointed out that both services, internal and external, operated under different legal frameworks. A lengthy debate – called by the Czech press 'the war of the secret services' – concerned the numbers and served to divert attention from the more important issues of political responsibility and functional ties to the respective ministries. Thus, when the new 'umbrella law' on the Intelligence Services of the Czech Republic[4] was finally approved by the parliament in July 1994, it codified the already existing structure with foreign intelligence being administered by the Ministry of Interior and the BIS being suspended in the executive vacuum, making functional ties with the Ministry of Interior (police) very complicated. On the other hand the acknowledgment of the existence and legitimacy of the two foreign intelligence services had a positive influence on the services' standing in the state apparatus and their relations with their counterparts abroad. The law also more clearly defined the accountability of the government and its respective Ministers for the activities of the services.

The law acknowledged the parliamentary powers of oversight, but did not go into greater detail. Instead, the government pledged another law which would be devoted solely to this matter and would clarify in great detail the parliament's oversight powers that would cover not only civilian and military counter-intelligence but also both civilian and military intelligence services. The Klaus government did not fulfil this promise and at least one good parliamentarian initiative in this regard (sponsored by Members of Parliament Oldřich Kužílek and Vladimír Šuman) was thwarted for reasons that had no bearing on the crux of the matter but were related to the squabbles within the ruling coalition. The opposition, consisting mainly of the Social Democrats, vowed to force the government to submit the much-needed law on oversight but did not succeed, even though one of the leading Social Democrats (Member of Parliament Jaroslav Bašta) became, in 1996, the head of the parliament's commission overseeing the BIS activities. In 1998, the Social Democrats came into power and Jaroslav Bašta became the Minister whose portfolio included, among other duties, coordination and

4 The full text of the act, no. 153 of 7 July 1994, can be found on the official website of the Czech Information Service, at: www.bis.cz/english/index.html.

legislation of the intelligence community. Several drafts of the law were made, but none of them found its way into parliament. Despite these legislative setbacks, the BIS and VOZ (civilian counter-intelligence and military counter-intelligence) parliamentary oversight commission, managed to push through certain changes in procedural matters such as parliament's power to lift the oath of silence from the officers. Therefore, in the second half of the 1990s the commission played a far more important role than it had in previous years.

The 1994 'umbrella law' was the last legislative measure pertaining to the Czech intelligence community adopted by the Czech parliament. When the Social Democrats formed their first government they vowed to learn from the mistakes committed by their right of centre predecessors and announced an ambitious plan that was to consist of two parts. Part one was supposed to be the audit and assessment of the activities of the Czech secret agencies. Logical follow-up to part one was supposed to be the reform of the community based on the results of the audit. The audit took place, but the results (for reasons not known to this author) were never revealed. The second phase of this bold plan, the reform that would repair the flawed architecture of the Czech intelligence community, has never materialised. Another social democratic promise to deliver to the parliament a draft of the law on parliamentary oversight has also not been fulfilled.

The events of 9/11 and their aftermath had two major impacts on the Czech intelligence community. The first is positive: both the Czech public and, hopefully, some of the politicians realised that spies and counter-spies do, at least from time to time, play a relatively important role in providing security in today's fragile world. Unfortunately, the events of 11 September also created an atmosphere in which any reformist plan will stay on the shelves for a long time to come.

## Conclusion

In the early 1990s, Czechs and Slovaks decided to make a clean break with the past. Most of the 'old intelligence structures' were removed and replaced with young recruits. This decision produced a huge psychological advantage in dealing with new western allies. It also served as an insurance against old communist skeletons coming out of closets at a time when the country least needed it. On the other hand, it takes a few years to train a good intelligence officer. The realisation was also reached that former dissidents usually do not make good spies and counter-spies. As the Czech intelligence community was coming of age, it had suffered some spectacular failures, registered a few considerable successes and had had its fair share of scandals, particularly in the mid-1990s. The laws covering the intelligence community were passed in haste and are in grave need of amendment. Oversight by the parliament only covers the activities of civilian and military counter-intelligence. It will take at least two years to include civilian and military intelligence under the parliamentary oversight umbrella. Despite its NATO and EU membership, the Czech Republic is still a country in transition and the state of the Czech intelligence community reflects the state of the whole society. It is neither better nor worse. I sometimes

wonder, would we be better off now if in the early 1990s we had tried to reform the already existing communist structures? Perhaps, but I strongly doubt it.

# PART III

# Reforms in the West

*This page intentionally left blank*

Chapter 7

# The United States Department of Defense Intelligence Oversight Programme: Balancing National Security and Constitutional Rights

*George B. Lotz, II*[1]

> Perhaps a day will dawn when tyrants can no longer threaten the liberty of any people, when the function of all nations, however varied their ideologies, will be to enhance life, not to control it. If such a condition is possible, it is in a future too far distant to foresee. Until that safer, better day, the democracies will avoid disaster, and possible total destruction, only by maintaining their defences.
>
> Among the increasingly intricate arsenals across the world, intelligence is an essential weapon, perhaps the most important. But it is, being secret, the most dangerous. Safeguards to prevent its abuse must be devised, revised, and rigidly applied. But, as in all enterprises, the character and wisdom of those to whom it is entrusted will be decisive. In the integrity of that guardianship lies the hope of free people to endure and prevail (Stevenson 2000, XVI).

## Introduction

This quote from Sir William Stephenson, in his book *A Man Called Intrepid*, succinctly captures why intelligence oversight is so important in a democratic society such as the United States. The American way of life is both defined and protected by our democratic political system. It is a system anchored in the Constitution, which established a republic characterised by significant limits on governmental power through checks and balances, a distribution of state and federal rights, and an affirmation of the rights and freedoms of individuals. Unfortunately, those checks and balances were not enough to prevent the misuse of US intelligence assets in the 1960s and 1970s. A period in which, in the name of

1. The author was the Assistant to the Secretary of Defense for Intelligence Oversight, US Department of Defense, from 1998-2005 during which time he wrote this chapter.

national security and domestic tranquillity, elements of the US government, including the military, stood accused of violating the very freedoms and liberties they were sworn to protect. How could this happen? And more importantly, to paraphrase Sir William Stephenson, what safeguards have been devised, applied and, as required, revised to prevent the misuse of intelligence assets in the future?

The Office of the Assistant to the Secretary of Defense for Intelligence Oversight (ATSD (IO)) was established as one of those safeguards. The Office was created with no constituency or vested interest, and reports directly to the Secretary and Deputy Secretary of Defense. The ATSD (IO) is charged with the independent oversight of all intelligence, counterintelligence, and intelligence-related activities in the Department of Defense (DoD). This responsibility covers the largest segment of the US intelligence community. In performing this critical function, and working in close coordination with the DoD General Counsel, the ATSD (IO) ensures that all activities performed by defence intelligence components are conducted in accordance with federal law, executive orders, DoD directives, regulations and policies.

There are several organisations that have been created to provide 'guardianship' over the US Intelligence Community. However, before addressing them, it is important to understand the events that led to their creation and how these organisations evolved – in particular the intelligence oversight process within the Department of Defense and the role of the ATSD (IO).

## Background

### *Turmoil and Unrest*

The 1960s were a period of turmoil and unrest throughout the United States. The period brought incidents of vocal dissent; large demonstrations; racial, political and campus violence; and, what some argued at the time, was 'the inauguration of a period of wide spread anarchy' (United States Senate 1978, p. 118). From 1964 to 1968, the US Army, acting as the Department of Defense executive agent for civil support, was increasingly called upon to help quell civil disturbances in a number of locations throughout the country. At first, the Army attempted to rely on the Federal Bureau of Investigation (FBI) and other civilian law enforcement agencies for what it deemed to be necessary information. However, when these agencies were unable to meet the information requirements, the Army turned appropriately to its own extensive resources and assets to collect the information required for specific events.

The military trains for how it plans to fight and fights as it has trained. But the military had not trained for this type of mission. Therefore, they began to apply the existing methods to preparing for and predicting future civil disturbances. These methods included the collection of more reliable intelligence information.

In February 1968, collection plans were drafted which targeted so-called dissident elements – specifically the anti-draft, anti-Vietnam War, and civil rights movements. As it was implemented, the scope of the collection effort expanded

nationwide and ranged from civil rights leaders to the leaders of the militant Students for a Democratic Society. Military counterintelligence units also provided an undercover presence at both the Democratic and the Republican National Conventions in 1968. Public scrutiny of these intelligence activities began in January 1970, with the publication of an article in the *Washington Monthly Magazine* entitled 'CONUS [Continental United States] Intelligence: The Army Watches Civilian Politics'. In his article, Christopher Pyle, a former Army intelligence officer, alleged that:

> Today the Army maintains files on the membership, ideology, programs, and practices of virtually every activist political group in the country. These include not only such violence-prone organisations as the Minutemen and the Revolutionary Action Movement (RAM), but such non-violent groups as the Southern Christian Leadership Conference, Clergy and Laymen United Against the War in Vietnam, the American Civil Liberties Union, Women Strike for Peace, and the National Association for the Advancement of Coloured People (Pyle, 1970, p. 5).

Mr. Pyle's article alleged that the expansion of the original DoD mission (what we now commonly refer to as 'mission creep') to support law enforcement agencies during periods of civil disturbance had resulted in 'the development of personality and organisational files on individuals and groups unassociated with violent political protests'.[2]

*Congressional Investigations*

As a result of this article, and the receipt of hundreds of letters and telegrams from members of Congress and other interested citizens urging an investigation and hearings to determine whether the charges were true, the Senate Subcommittee on Constitutional Rights, Committee on the Judiciary, chaired by Senator Sam Ervin, conducted hearings in February and March 1971 on the military surveillance of civilians.

After an exhaustive review, lasting over three years, the Subcommittee concluded that:

2. The Report Military Surveillance of Civilian Politics of the Subcommittee on Constitutional Rights Committee of the Judiciary United States Senate, 93 Cong., 1st Sess., noted that the Pyle article reported 'the Army's data collection had its origins in the Army's preparation for riot duty but had gone beyond the need for reconnaissance of cities to the development of personality and organisational files on individuals and groups unassociated with violent political protest'. According to Mr. Pyle, as quoted in the Committee Report, this information was to be compiled in a computerised data bank. The Committee Report stated that Mr. Pyle alleged that what made the data bank unique was its devotion 'to the storage of information about the primarily lawful activities of civilians unaffiliated with the Armed Forces' (United States Senate, 1978).

> Army surveillance of civilians engaging in political activities in the 1960s was both massive and unrestrained. At the height of the monitoring, the Army engaged over 1,500 plain-clothes agents to collect information, which was placed in scores of data centres around the country. While most of the information collected consisted of activities such as the clipping of newspaper accounts and attending public events, there were many more serious instances of surveillance in which covert means were used to observe or infiltrate groups. No individual, organisation, or activity which expressed 'dissident views' was immune from such surveillance and, once identified, no information was too irrelevant to place on the Army computer (United States Senate, 1978, p. 4).

The Subcommittee found that much of the surveillance had been justified by the military on the suspicion that the disorder and civil unrest could be attributed to a wide-spread conspiracy (United States Senate, 1978). In concluding that Army surveillance was both unauthorised and in violation of the First Amendment, the Subcommittee stated:

> What had taken place was not so much a conscious effort to subvert the freedoms of speech and association, as it was a classic example of a burgeoning bureaucracy going out of control, with no direction and no limitations. What began as a limited intelligence activity by individual commands responding to the military's limited need for information for use during civil disturbances mushroomed into an elaborate, nationwide system with the potential to monitor any and all political expression (United States Senate, 1978, p. 117).

Other investigations were soon to follow the work of the Subcommittee. In July 1975, the Senate Select Committee to Study Governmental Operations, chaired by Senator Frank Church, began a much broader investigation of intelligence abuses that included the activities, both at home and abroad, of the Central Intelligence Agency (CIA). The Committee's investigation resulted in an exhaustive fifteen-month endeavour. Altogether the Committee conducted over 800 interviews of individuals, held 126 full committee meetings, held 40 subcommittee meetings, held 250 executive hearings, conducted 21 days of public hearings, amassed 10,000 pages of documentation, released to the public 14 volumes of hearings and reports, and made 183 recommendations to the Senate. For the first time in American history, public hearings were conducted on the innermost workings of US intelligence. Agency Directors and personnel were compelled to testify under the glare of television lights (Smist, 1990, cited DIA [Defence Intelligence Agency], 1997, p. 4). Despite its extensive findings and recommendations, the Church Committee made no legislative proposals. However, it did recommend that a follow-on committee in Congress consider additional legislation should the need become apparent (United States Senate, 1994, p. 5).

The US House of Representatives Select Committee on Intelligence, chaired by Representative Otis Pike, also began an investigation of intelligence activities in 1975. However, troubles plagued the Pike Committee and it never published a final report. The only official output of the Pike Committee ever released by the House of Representatives was a list of recommendations published on 11 February 1976

(House of Representatives 1994). Two of the Committee recommendations were that: (1) the intelligence components of the armed services be prohibited from engaging in covert action within the United States. It further recommended that clandestine activities against non-military US citizens abroad be proscribed; and (2) the establishment of an Intelligence Inspector General (IG). The IG would have the authority to investigate any possible or potential misconduct on the part of the various intelligence agencies or personnel therein.

The investigations by the Ervin, Church, and Pike committees uncovered clear evidence of extensive wrongdoing that had been perpetrated by many elements of the US intelligence community. A number of abuses against private American citizens was confirmed, including the illegal reading of private mail by the CIA; the existence of over a 1,000,000 unauthorised CIA and FBI files on individuals; electronic eavesdropping on private telephone conversations by the National Security Agency; 100,000 unauthorised background investigations by Army intelligence units; and the unauthorised release of individual tax records by the Internal Revenue Service (IRS) (Johnson, 1989, cited DIA, 1997, p. 5). The Congress concluded that the CIA had also conducted drug experiments on unsuspecting subjects, in addition to infiltrating a number of religious, media, and academic organisations, manipulating foreign elections, and making at least two unsuccessful attempts to assassinate foreign leaders (Johnson, 1989, cited DIA, 1997, p. 5). When these findings were released, they created tremendous public pressure for reform of the CIA and other elements of the intelligence community.

The revelations, conclusions, and recommendations of the committees resulted in new rules and procedures for US intelligence agencies meant to inhibit abuses of authority while preserving intelligence capabilities. Equally important, the investigations identified the need for a concerted effort by the legislative, judicial, and executive branches if a balance was to be maintained between the country's need for intelligence and its need to protect core individual rights. Finally, the Congressional investigations and recommendations confirmed the role of the media in intelligence oversight as a catalyst for change.

*Congressional Response*

The Congressional inquiries and investigations that marked this period clearly represented a watershed for the US intelligence community. Responding to public pressure and their own concerns over past abuses, both the House of Representatives and the Senate resolved to strengthen their oversight of intelligence activities and the intelligence community. The key ingredient in this process was the creation of the Senate Select Committee on Intelligence and the House Permanent Select Committee on Intelligence to perform ongoing oversight of US intelligence activities. Congress also considered, although ultimately rejected, laws designed specifically to regulate the conduct of intelligence activities.

This changed when Congress enacted the Foreign Intelligence Surveillance Act, Public Law 95–115, 1978. This Act created a procedural structure with a special federal court for considering and approving, in secret, certain surveillance

activities that occur in the US and thus have the potential to affect rights guaranteed under the Constitution. Prior to the court's creation, warrantless electronic surveillance of foreign powers and their agents was based on the President's inherent and constitutional powers as the chief executive officer and commander-in-chief of the armed forces, and his responsibilities to conduct the nation's foreign affairs.

*Presidential Action*

In 1976, President Gerald Ford, in response to the Pike Committee recommendations (that had been released just one week earlier) and in anticipation of the upcoming Church Committee report (which would be released within several months), issued Executive Order 11905, 'United States Foreign Intelligence Activities (1976)'. The Executive Order outlined a number of specific restrictions on US intelligence activities. It also created (1) the President's Intelligence Oversight Board (PIOB) to monitor the conduct of intelligence components; and (2) the Committee on Foreign Intelligence (comprised of the Deputy Secretary of Defense, the National Security Advisor, and the Director of Central Intelligence (DCI)) to establish policy priorities for the management of the National Intelligence Program and to oversee the development and allocation of intelligence budget resources. The Executive Order was the first unclassified directive on US intelligence roles and responsibilities (all prior direction and guidance had come exclusively from classified National Security Council directives) (DIA, 1997).

Executive Order 11905 tasked those federal agency Inspectors General and General Counsels, having oversight responsibilities for activities within the Intelligence Community, with the additional responsibility for discovering and reporting to the PIOB activities raising questions of legality and propriety. As a result, the DoD established the Inspector General for Intelligence on 30 June 1976. This new office was assigned responsibility for the independent oversight of all defence foreign intelligence and counterintelligence activities to ensure compliance with laws and standards of propriety.[3]

The administration of President Jimmy Carter sought to continue the building process started under President Ford. Its goal was the establishment of a clear legal framework for US intelligence activities by working at two levels: first, by drafting a new Executive Order; and second, in consultation with the two newly-formed Congressional oversight committees, by developing legislation to establish in law the mission and functions of US intelligence agencies (United States Senate 1994, p. 5).

President Carter, prior to a comprehensive intelligence charter, signed Executive Order 12036, 'United States Intelligence Activities', in January 1978. It

3. The IG/DI's Charter Directive was reissued on December 23, 1980; it changed the position title to the Inspector General for Intelligence (IG/I), and referenced EO.12036, signed by President Carter. However, there were no substantive changes to the IG/I's functions.

superseded President Ford's Executive Order 11905. President Carter issued this Executive Order to further define the roles and responsibilities of the major components of the intelligence community, while maintaining most of the restrictions on activities established by EO 11905. Several of the new Executive Order's provisions were the result of a close interface between the Congressional intelligence committees, working on new intelligence legislation, and the DCI's staff. Reflecting this close relationship were the restrictions set forth in the Executive Order that were intended to ensure that US intelligence officers respect the rights of United States persons. As President Carter stated at the signing of the Order:

> I believe that this Executive Order represents an important step forward in assuring the American people that their intelligence agencies will be working effectively for them and not infringing on their legal rights.

Among the most important provisions of Executive Order 12036 was a requirement that the restrictions on intelligence gathering contained in the Order be implemented by regulations in each intelligence agency that had been approved by the United States Attorney General. This requirement not only assured consistency in approach throughout the intelligence community but also provided legal review, external to intelligence agencies, of the rules governing their activities (United States Senate 1994, p. 5). The Executive Order also mandated that the DCI and the heads of the intelligence agencies keep the two Congressional intelligence committees 'fully and currently informed of intelligence activities', including 'significant anticipated intelligence activities', and to provide pertinent information in their possession to the oversight committees – subject to the constitutional authorities of the President and the statutory duty of the DCI to protect intelligence sources and methods. This was the first binding direction to intelligence agencies to cooperate with the Congressional oversight committees.

When President Ronald Reagan took office, one of his primary goals was to reduce bureaucratic constraints whenever possible, consistent with law (United States Senate 1994, p. 21). The Reagan Administration wanted to give intelligence officers a clear signal that it recognised the value and importance of an effective intelligence programme and that it had confidence in the men and women of the various components of the intelligence community.[4]. President Reagan's Executive Order 12333, 'United States Intelligence Activities', superseded EO 12036, in December 1981, and is still in force today. It provides greater latitude than its predecessor, both in what may be collected on US persons and how it may be collected. For example, section 2 of EO 12036, 'Restrictions on Intelligence Activities' became 'Conduct of Intelligence Activities' in EO 12333. In addition, E.O. 12333 redefined the meaning of a US person, for example, an alien is no longer considered a US person unless the individual is known to be a permanent

4. Quoted by Major General Jack E. Thomas, USAF (retired), and 'EO 12333 - Analysis & Fact,' internal OSD ASD/C3I talking paper, 1982.

resident. The term also does not include corporations directed and controlled by a foreign government or governments.

In addition to EO 12333, there is another Executive Order that provides a mechanism for the oversight of the US intelligence community. In September 1993, President Bill Clinton issued EO 12863, 'President's Foreign Intelligence Advisory Board (PFIAB)', which is still in effect today. President Eisenhower originally established the PFIAB in 1956.[5] For forty years the PFIAB had served as an independent body providing the President with objective, expert advice on the conduct of US intelligence activities. In 1976 President Gerald Ford created the Intelligence Oversight Board (IOB). The mission of the IOB is to advise the President on the legality of intelligence activities. EO 12863 merged the two bodies, with the IOB becoming a standing committee of the PFIAB. Under EO 12863, the mission of the PFIAB is to:

> … enhance the security of the United States by improving the quality and effectiveness of intelligence available to the United States, to assure the legality of activities of the intelligence community ….

A unique feature of the PFIAB is its composition:

> The PFIAB shall consist of not more than 16 members, who shall serve at the pleasure of the president and shall be appointed by the president from among trustworthy and distinguished citizens outside the government who are qualified on the basis of achievement, experience and independence (Executive Order 12863, section 1.1).

The membership of the IOB is drawn from the PFIAB. Its duties are as follows:

(a) prepare for the President reports of intelligence activities that the IOB believes may be unlawful or contrary to executive order or presidential directive;
(b) forward to the Attorney General reports received concerning intelligence activities that the IOB believes may be unlawful or contrary to executive order or presidential directive;
(c) review the internal guidelines of each agency within the intelligence community that concern the lawfulness of intelligence activities;
(d) review the practices and procedures of the Inspectors General and General Counsels of the intelligence community for discovering and reporting intelligence activities that may be unlawful or contrary to executive order or presidential directive; and
(e) conduct such investigations as the IOB deems necessary to carry out its functions under this order (Executive Order 12863, section 2.2).

Executive Orders 12333 and 12863 are integral to the intelligence oversight of the members of the US intelligence community, including the Department of Defense. However, intelligence safeguards in the Department of Defense preceded the very first Executive Order issued by President Ford.

5. It was originally called the President's Board of Consultants on Foreign Intelligence Activities. It gained its current name under President Kennedy and it has served all presidents since that time except for President Carter.

**Evolution of Department of Defense Intelligence Oversight**

Prior to the conclusion of, and in some cases preceding, the aforementioned Congressional inquiries, the DoD took steps to impose severe restrictions on surveillance of US persons. This effort included the destruction of information already contained in defence files and the establishment of a structure to regulate future departmental intelligence activities which included the creation of an oversight programme to curb unrestricted and uncontrolled domestic surveillance. In December 1970, the Army issued several guidance letters on domestic surveillance. These letters were intended to regulate all counterintelligence activities directed against civilians not associated with the Defence Department (United States Senate 1978, p. 92). In the letters, the Army identified specific situations where collection would be warranted.[6] In the same month, Secretary of Defense Melvin Laird issued his own order in which he declared that the Secretary of Defense was assuming control of all military intelligence, both foreign and domestic (United States Senate 1978, p. 94).

In March 1971, the DoD issued Department of Defense Directive 5200.27, 'Acquisition of Information Concerning Persons and Organisations not Affiliated with the Department of Defense'. In large part, this Directive was based upon both Secretary Laird's order and the Army policy letters. Its central tenet was that military intelligence should not monitor the political activities of civilians unaffiliated with the Department of Defense except in narrowly defined situations, and should not participate in the collection of civil disturbance information unless (1) the Justice Department fails to provide it, (2) the Secretary of Defense (or his designee) finds a distinct threat of civil disturbance exists, and (3) he, accordingly, authorises the collection activity (United States Senate 1978, pp. 94–95).

6. DoD Directive 5200.27 (United States Senate 1978, p. 92). Situations warranting the collection of information on civilians by any means, including infiltration, are limited to:
   (1) attempts to subvert loyalty, discipline, or morale of Department of Defence military or civilian personnel by actively encouraging desertion, disobedience, of lawful orders or regulations, or disruption of military activities.
   (2) theft of arms, ammunition, or equipment, or destruction or sabotage of facilities, equipment or records belonging to Army units or installations.
   (3) threats to the security of Army elements or operations or to classified Defence information through espionage on behalf of any recipient, foreign or domestic.
   (4) unauthorised demonstrations on active duty or reserve Army installations or through demonstrations immediately adjacent to them, which are of such a size or character that they are likely to interfere with the conduct of military activities.
   (5) threats of physical violence to Department of Defence military or civilian in connection with their physical activities.
   (6) threats to the physical safety of governmental officials who have been authorised protection by Army resources.
   (7) threats of sabotage or espionage directed against Federal installations for which the Army has been delegated Department of Defence responsibility.

During this period, Secretary Laird also directed the creation of the Defense Investigative Review Council (DIRC) to ensure that DoD investigative units were in strict compliance with the departmental policy contained in the new Directive ('Federal Data Banks, Computers and the Bill of Rights' cited United States Senate 1978, p. 395). The Council was chaired by the Assistant Secretary of Defense for Administration, and included the DoD General Counsel, the Under-Secretaries of the Army, Navy, Air Force and the Director of the Defense Intelligence Agency. The DIRC charter stipulated that it would ensure defence investigative and counterintelligence (CI) missions were consistent with individual constitutional rights and legal provisions.[7]

The DIRC, which existed from 1972 through 1976, conducted 21 unannounced inspections of military investigative units in the field. Through review of unit files and interviews with unit personnel, the DIRC teams focused on several areas in their inspections:

- Awareness: Were the inspected units aware of defence guidance on collection of information?
- Compliance: To what extent had the inspected units complied with the guidance?
- Impact: What was the impact of the guidance upon their mission?
- Liaison: What was the nature of the inspected unit's relationship with civilian law enforcement organisations? What type of information was being exchanged and what type of assistance was being requested/provided?

In addition to its own oversight functions, DIRC policy guidance required that the Secretary of each military service be responsible for the oversight of their domestic intelligence and counterintelligence activities as well. Each service Secretary was required to provide an annual report to the Secretary of Defense, through the DIRC Chairman, on the activities of his units.

In 1976, in response to President Ford's EO 11905, then and current Secretary of Defense Donald Rumsfeld terminated the DIRC, and established the Inspector General for Intelligence (IGI) in the Office of the Secretary of Defense. In 1982, with the statutory establishment of the DoD Inspector General (IG), a decision was made to maintain the intelligence oversight function separate from the IG and redesignate the IGI as the Assistant to the Secretary of Defense for Intelligence Oversight.

---

7. In consideration of the limits of its jurisdiction the DIRC noted, in an October 27, 1971 final working group draft of Study Report No. 10, that:
   Consideration has been given to extending DIRC policies into the area of foreign intelligence operations. It is believed that the widest range of flexibility of operations is required in this area and there are no sufficient countervailing reasons to warrant consideration of constraints in this area.

Since this office's inception, two things have remained constant: (1) because of the importance of intelligence oversight, this office has remained an independent organisation reporting directly to the Secretary and Deputy Secretary of Defense; and, (2) the fact that its goal is to ensure intelligence oversight policies are carried out by DoD intelligence units and non-intelligence units performing intelligence activities. These policies are based on both the US Constitution and EO 12333.

*Implementing Executive Order 12333 within the Department of Defense*

As the operative guidance on the conduct of intelligence activities by US intelligence components, Executive Order 12333 requires the National Security Council, the Secretary of Defense, the Attorney General, and the Director of Central Intelligence to issue 'such appropriate directives and procedures as necessary to implement this Order' (Executive Order 12333 1981, section 3.2). In addition, section 2.3 of the Order clarifies that:

> Agencies within the intelligence community are authorised to collect, retain, and disseminate information concerning United States persons only in accordance with procedures established by the head of the agency concerned and approved by the Attorney General …

As a result, Department of Defense Regulation 5240.1-R, 'Procedures Governing the Activities of Defence Intelligence Components that Affect United States Persons' which implements EO 12333 within the Department of Defense, was signed and approved jointly by the Secretary of Defense and the Attorney General in 1982.

*The Department of Defense Procedures*

Department of Defense Directive 5240.1, 'DoD Intelligence Activities', signed in April 1988 (see Executive Order 12333, 1981), requires that all defence intelligence activities be conducted in strict conformity with the US Constitution, applicable law, Executive Order 12333 and DoD 5240.1-R, with special emphasis given to protection of the constitutional rights and privacy of US persons. It also directs the Assistant to the Secretary of Defense for Intelligence Oversight to (1) serve as the central focal point for all contacts with the President's Intelligence Oversight Board; and, (2) to perform the function of intelligence oversight. The intelligence oversight duties are outlined in DoD Directive 5148.11, 'Assistant to the Secretary of Defense for Intelligence Oversight (ATSD [IO])' which states:

> ... the ATSD (IO) shall ensure that all activities performed by intelligence units and all intelligence activities performed by non-intelligence units, are conducted in compliance with Federal law and other laws as appropriate, Executive Orders and Presidential Directives, and DoD Directives System issuances.

The key 'DoD Directives System issuance' is DoD Regulation 5240.1-R, 'Procedures Governing the Activities of Defense Intelligence Components that Affect United States Persons'.

The regulation contains 15 procedures that address specific subject areas, the majority of which are based on EO 12333. Procedure 1 of the General Provisions, clarifies that the regulation only applies to intelligence components. In addition, it does not apply to law enforcement activities, including civil disturbance activities that may be undertaken by DoD intelligence components. And of special significance, it forbids DoD intelligence components from requesting any person or entity to undertake any activity forbidden by the Executive Order. Procedures 2–4 of the regulation provide 'the sole authority' by which intelligence components may collect, retain and disseminate information concerning US Persons. Procedures 5–10 set forth guidance with respect to the use of certain collection techniques. Procedures 11–13 address contracting for goods, assistance to law enforcement, and human experimentation for intelligence purposes. Procedures 14 and 15 address intelligence oversight requirements. The Defense Department requires all employees of DoD intelligence components to be familiar with Procedures 1–4, 14 and 15.

Procedures 14 and 15 address the responsibilities of the intelligence professional, their legal advisors, inspectors general, and their command structure, and represent a critical safeguard. Employee conduct, which is addressed by Procedure 14, requires that defence intelligence component employees conduct themselves in accordance with the regulation. In addition, intelligence components are required to familiarise their personnel with the provisions of the regulation as its provisions pertain to the employee's duties. Procedure 15 requires all intelligence component employees to report any questionable activity to that component's general counsel or inspector general, to the Defense Department General Counsel, or to the ATSD (IO). A questionable activity refers to any professional intelligence conduct that may violate the law, any Executive Order or presidential directive, including EO 12333, or applicable defence policy, directive or regulation including this regulation. Together these procedures establish an expectation in all defence intelligence personnel and intelligence components, that intelligence oversight is their responsibility – one for which they will be held accountable.

**Intelligence Oversight in the Department of Defense Today**

The purpose of the defence intelligence oversight programme is to ensure the proper balance between the acquisition and use of essential information by the intelligence community, and the protection of statutory rights and those guaranteed by the US Constitution. Heads of intelligence units, their commanders, judge advocates general, inspectors general, and intelligence professionals are all partners in ensuring the integrity of the intelligence oversight process. The Assistant to the Secretary of Defense for Intelligence Oversight manages this process.

The ability to maintain a proper balance between national security needs and constitutional freedoms is being challenged by threats highlighted by the terrorist attacks of 9/11. Key to maintaining this proper balance are many of the goals and methodologies first established by the DIRC and currently employed by the defence intelligence oversight programme. The programme has three principal, but highly complementary, objectives: awareness, education, and training; compliance and prevention; and, development of tailored policy guidance.

The keystone of the defence intelligence oversight programme is awareness, education, and training. It has been almost 30 years since the findings of the Church Committee were published. Unless intelligence professionals understand how the misuse of intelligence assets occurred in the 1960s and 1970s, history could repeat itself, especially with the heightened security concerns in the United States today. Intelligence personnel and their leadership need a solid understanding of why EO 12333 and DoD Regulation 5240.1-R exist. In addition, they need to understand the mission of the unit in which they are assigned. Drawing from this foundation, they will then understand why they are authorised to perform certain missions, but not others – even when they have the technical capability. These lessons are then continuously reinforced through on-going training. Units that have active intelligence oversight training programmes rarely have problems. When questions arise that their intelligence oversight officer cannot answer they know they can turn to their legal advisor. We can develop an appreciation for the importance of protecting the statutory and constitutional rights of US persons by ensuring understanding of the activities that intelligence organisations and personnel may, and may not, lawfully perform – and, most importantly, the reasons why these limits exist.

To this end, a new DoD intelligence oversight training programme has been developed. The programme is adaptable to fit the specific needs and requirements of all Defense Department intelligence components. This computer-based multimedia training programme is available on DoD classified networks as well as on stand-alone computer systems using compact discs. Because the mission and requirements of each defence intelligence component may vary, necessitating greater emphasis and focus on specific areas, the programme permits the inclusion of tailored training modules on intelligence oversight issues, challenges, questions and answers for functional areas of intelligence. Training also includes a self-evaluation tool for individuals to assess their knowledge and to record and account for completion of training to appropriate intelligence oversight officials. This

system will not replace, but rather will complement, the current ATSD (IO) website (www.dod.mil/atsdio), which provides background, history, reference material, and other information on intelligence oversight to intelligence personnel and to the general public.

Intelligence oversight inspections and staff assistance visits by the ATSD (IO) to DoD intelligence components will continue to test the knowledge of intelligence personnel on basic intelligence oversight procedures. In addition, these inspections perform an equally important function of educating the inspectors on changing missions and capabilities of the units. In special cases, they may also act as the catalyst for intelligence oversight policy changes or revised guidance necessary to accommodate new capabilities and/or missions. However, this is not the only avenue for change. When prevention fails and violations occur, intelligence oversight officers must identify, investigate, and report violations, through their chain of command, to the ATSD (IO).

The ATSD (IO) is authorised to direct DoD components to investigate allegations of illegal or improper activities by their intelligence elements. The ATSD (IO) reviews and analyses reports of questionable activities received from defence intelligence components, the General Counsels, and the Inspectors General of the Joint Staff, Military Services, Combatant Commands, and the defence intelligence agencies. Questionable activities of a serious nature are reported to the Secretary of Defense and the President's Intelligence Oversight Board. They may also be referred to the Department of Justice, if warranted. In addition, at the direction of the Secretary of Defense, upon request of other senior defence officials, or on his own initiative, the ATSD (IO) may also conduct special inquiries into allegations of questionable or improper activities by defence intelligence components. The results of these inquiries are also reported to the Secretary of Defense and the President's Intelligence Oversight Board.

Each General Counsel and Inspector General of a defence intelligence component is required to submit an intelligence oversight report, each calendar quarter, to the ATSD (IO). The reports describe significant intelligence oversight activities performed by their units, as well as questionable activities and corrective actions taken with respect to such activities. Significant items that merit the attention of the President's Intelligence Oversight Board are addressed and forwarded in the Defense Quarterly Intelligence Oversight Report, prepared by the ATSD (IO), and signed jointly by the ATSD (IO) and the Defence Department General Counsel. The Report is approved by the Secretary of Defense and delivered to the President's Intelligence Oversight Board.

A critical aspect of evaluating reports of intelligence oversight violations and irregularities is to discover their source, that is, what led to the situation. The ATSD (IO) approach is to evaluate these events from a holistic perspective. This means evaluating everything from training to DoD policy guidance. In some cases, DoD policy guidance may not adequately address newly evolving missions and capabilities, thus causing a technical violation to occur. It is the responsibility of the ATSD (IO) to ensure that DoD policy guidance stays current with evolving missions and capabilities to ensure the proper balance between national security needs and constitutional freedoms.

Through the implementation and constant improvement of an aggressive intelligence oversight programme that incorporates training, inspections and investigations, DoD intelligence professionals are acutely aware of their intelligence oversight responsibilities. Annual training on the intelligence oversight procedures and policies has given DoD intelligence professionals the ability to collect, retain and disseminate intelligence information with confidence that their actions are in accordance with US law and policy. While questionable intelligence activities periodically occur, the combination of training, followed up by prompt investigation and aggressive follow-on inspections, have insured that these violations and questionable activities have not become systemic.

*Intelligence Oversight Outreach Program*

The ATSD (IO) has established an Intelligence Oversight Outreach Program. It currently has two parts. The first is to make senior military and civilian leaders in the Defense Department better aware of intelligence oversight, so that they are able to provide the appropriate leadership and guidance to those intelligence professionals supporting them. Better-informed leadership will make for better intelligence support to commanders.

The second portion of this outreach programme involves providing intelligence oversight information to middle and senior military leaders of emerging democracies around the world. The ATSD (IO) currently presents programmes at the George C. Marshall European Centre for Security Studies in Germany; to current and future military and civilian leaders of nations in Central and Eastern Europe; and to middle- and senior-level leaders, including those from newly joined member nations, at the North Atlantic Treaty Organisation School in Germany. These programmes provide the participants an opportunity to participate in role-playing with real-world scenarios in order to reinforce what they have learned. The goal of these programmes is to impart to the students participating in the sessions a basic appreciation and understanding of intelligence oversight so that when they are in leadership positions, within their respective countries, they might see the merits of incorporating similar safeguards into their own intelligence structures.

## Conclusions

Grappling with the aftermath of the terrorist attacks of 9/11, the words of Sir William Stephenson (2000) take on a particular meaning and urgency for intelligence organisations: ‘Safeguards to prevent (its) abuse must be devised, revised, and rigidly applied’.

Homeland security is the latest and most important of a multiple array of national security priorities that face the Defence Department, such as computer security, cyber attacks, and international narcotics trafficking. As intelligence capabilities continue to improve and expand, they will play an increasing role in the formulation of the US response. The intelligence oversight programme also

continues to evolve so that it can provide effective safeguards to the changing issues and challenges that face defence intelligence personnel. As the ability to acquire and process intelligence information grows, intelligence personnel must be able to recognise when these capabilities have the potential to endanger our constitutional freedoms; and it is then leadership that determines what preventive or corrective steps need to be taken. Intelligence oversight in the Department of Defense is a collaborative effort. It works best when collectors and consumers of intelligence information understand and appreciate the delicate balance between security and personal freedoms that must be maintained. When this partnership occurs, the 'integrity of that guardianship' is secure.

Chapter 8

# Checks and Imbalances? Intelligence Governance in Contemporary France

*Hans Born and Thorsten Wetzling*[1]

## Introduction

French intelligence services are both renowned and feared for their special alertness. This reputation is now particularly well established in matters of counter-terrorism, an area of government where, until two decades ago, French politicians deplored that the country '… was paying for years of indifference, irresponsibility, and laxity in the face of the problem of international terrorism' (Favier and Martin-Roland, 1991, p. 175). Admittedly, much has changed since then. France is now deemed to pursue 'one of Europe's most effective and aggressive counterterrorism policies' (US Department of State, 2005). This transformation has many causes, some of which will be briefly mentioned here. France encountered Islamic international terrorism earlier than other western democracies.[2] Consequently, the country had to think and prepare for responses that few other democracies had considered at that time. By the end of the 1980s, the often deplored laxity towards threats to French security gave way to zealousness in counter-terrorism activity.

Throughout the last few years, the French intelligence services have been praised for having 'scored notable successes in preventing planned terrorist attacks' (Shapiro and Suzan, 2003, pp. 67–98). Yet, by comparison, contemporary France grants suspected terrorists fewer rights than other democracies: it permits interrogation without the presence of a lawyer, lengthy pre-trial incarcerations, and evidence acquired under questionable circumstances (Pipes, 2005). The apparent success in thwarting terrorist attacks is also often linked to the measures that were introduced to reform the intelligence apparatus. Notably, these measures were enacted on the basis of government decrees rather than by adopting intelligence

1. The authors would like to thank Mr. Antoine Garapon, Executive Secretary of the *Institute des Hautes Etudes sur la Justice*, Paris (HEJP) for his constructive remarks on an earlier version of this text.

2. One could point to the series of terrorist attacks that plagued the city of Paris during the summer of 1986, see Shapiro and Suzan, 2003, pp. 67–98.

laws through a democratically elected parliament.[3] With a view to the most relevant French intelligence and security services, it is perhaps less surprising that some of them (for example, the *Direction Centrale des Renseignements Généraux* – DCRG) are bestowed with mandates which generally exceed what most democracies have been prepared to grant to their respective services.[4] What is more, France displays an unusually high level of cooperation between the judiciary and the intelligence services. This practice has a very pragmatic appeal and is also reputed to have profoundly contributed to the efficiency of French counter-terrorism (Garapon, 2005). Unfortunately, equally important aspects, such as the constitutional legality of some of these collaboration practices, tend to be eschewed. Exemplary for this attitude is the famous French terrorist hunter, Judge Jean-Luis Bruguière, who makes no secret about where he has assigned his priorities. For him what really matters is that 'none of the nineteen 9/11 hijackers, who came from Spain, Belgium, Germany and Great Britain, had dared to step on French soil' (Mönniger, 2004).

Despite this accomplishment, something is wrong in the state of France. This chapter aims to assess the democratic merit of French intelligence governance. In the face of growing calls from French citizens, scholars, parliamentarians and intelligence staffers for a more rigorous and transparent system of intelligence control (Quiles 2000; Le Sénat, 1999; L'Assemblée Nationale, 1999), concrete steps in this direction, most notably through the establishment of a parliamentary intelligence oversight committee, have yet to be taken.[5] Our argument begins by introducing the concept of intelligence governance as the underlying yardstick for our analysis.

## A Normative Approach for Reviewing the Intelligence System of France

Decisions involving national security are among the most difficult and consequential ones in any democracy. How to strike a fair balance between the commitment to security and democracy? How can France secure the effectiveness of its intelligence and security services while holding them accountable and within the rule of law? It is in response to these questions that the concept of *democratic intelligence governance* is of great service. In essence, this concept combines the logics of the established principle of *good governance* and the notion of a *democratic security sector*. Both aspects need explanation. With regard to good governance, one needs to point out that 'government' differs from 'governance'.

3. In this regard we point to Decree # 82–306 (April 1982), Decree # 82–1100 (December 22, 1982), Decree # 92–523 (June 16, 1992), Decree # 98–608 (July 17, 1998) which provided the legal basis for the French intelligence and security services. See Table 8.1.
4. For further information about the mandates of intelligence services in other democracies, see Born, Johnson, and Leigh, 2005.
5. See below for an account of recent developments towards the creation of a French parliamentary intelligence oversight committee.

'Governance is more encompassing than government; it helps to grapple with the complex reality of the contemporary world in which governments are still central actors in domestic and international affairs though they increasingly are seen to share authority with non-state actors on multiple levels of interaction' (Hänggi, 2003, pp. 6–7). Governance is very much process orientated, the core element of this principle necessitates that government is people-centred, equitable, accountable, transparent, engenders participation and consultation in planning and decision-making, is effective and efficient in public sector management, and actively seeks and facilitates the involvement of civil society (World Bank, 1994).

The notion of a democratic security sector draws directly on the requirements of good governance. Civilian actors play a more prominent and integrated role in a nation's security architecture which can be demonstrated by the five constitutive pillars of a democratic security sector, namely: (a) organisations authorised to use force, (b) civil management and oversight bodies, (c) justice and law enforcement institutions, (d) non-statutory security forces, (f) non-statutory civil society groups (UNDP, 2002, p. 87). All in all it can be said that the overarching goal behind good governance of any nation's security/intelligence sector is the attempt to insulate the services from political abuse while acknowledging, and actively facilitating, their crucial role in the democratic state (Born and Leigh, 2005, p. 13).

## The French Intelligence Sector

To begin, one needs to be clear about intelligence. Do we have a clear definition for it? What is more, is intelligence universally understood in the same way? The answers to both questions are negative. There exists no single accepted definition of intelligence. Despite being one of the oldest professions in the world this is not entirely surprising. Given that national customs differ regarding this highly secretive trade one would also need to ask whether one can realistically expect a clear definition. The French word *renseignement* does not easily lend itself to be translated into 'intelligence'.[6] Observers of French security politics often point out that intelligence services like the British MI5 or the American CIA do have a French counterpart but that French security and intelligence agencies in general are much better understood by adopting a country-specific historical perspective rather than an Anglo-Saxon understanding of 'intelligence'. While it is true that intelligence means different things to different regions and different regimes, it must not be forgotten that in a globalised world with increased intelligence cooperation among democratic countries (be it in international counter-terrorism efforts or joint-military operations) a shared understanding about the nature of intelligence and its standards is indispensable. In the absence of a universal definition of intelligence, a widely shared understanding of intelligence is less difficult to construe. Mark Lowenthal reminds us that intelligence is several things:

6. Information or Inquiry would be the more suitable translation.

it is information, process and activity, and it is performed by lawful authorities, that is by nation-states (Warner, 2002). He maintains that:

> … intelligence is the process by which specific types of information important to national security are requested, collected, analysed, and provided to policymakers; the products of that process; the safeguarding of these processes and this information by counterintelligence activities; and the carrying out of operations as requested by lawful authorities (Lowenthal, 2002, p. 8).

## The Services

In France, the main ministries concerned with security and defence issues, that is, the interior, justice, foreign affairs, defence, science and technology, trade and communication ministries, have each their own intelligence structures (Faupin, 2002, p. 4). In the face of a plethora of different intelligence agencies, it is helpful to categorise the services as external security, internal security, and military intelligence agencies. Albeit itself an imperfect approach, this enables us to present the system in a more coherent manner.[7] Furthermore, one can further distinguish between the security and intelligence services which are under the formal authority of the French Ministry of the Interior (MoI), the French Ministry of Defence (MoD) and the institutions that respond to the office of the French Prime Minister.

Beginning with the services under the MoI, both the *Direction de la Surveillance du Territoire* (DST) and the *Direction Centrale* des *Renseignements Généraux* (DCRG) should be briefly mentioned. The DST, France's renowned internal security agency, detects and prevents activities on French territory likely to threaten France's security. Whereas the detailed organisation of the DST is classified information, it is common knowledge that the organisation consists of a central administration in Paris and seven regional directorates plus units installed in French overseas territories. Since the end of the Cold War, the tasks of the DST are concentrated in three areas: counter-espionage, counter-terrorism and espionage activities in economic, scientific and technical domains.[8] Whereas the division of tasks between external intelligence agencies and the DST is similar to the MI5/MI6 or CIA/FBI division in Britain and the US, 'the French secret services have a third dimension which attracts little attention but which is a source of significant controversy within France – a panoply of services unprecedented in a democracy which focus on the collection of domestic intelligence, the most prominent of which is the *Direction Centrale des Renseignements Généraux*' (Porch, 1995, p. 423). The controversy around the DCRG has to do with its mandate: it is tasked with research and centralisation of information 'intended for the information of the

7. It is not perfect as external intelligence services often take on traditional tasks of military agencies and criminal intelligence agencies often take on traditional tasks of internal security services – and vice versa.
8. See website of the French Interior Ministry 'La direction de la surveillance du territoire', available at: http://www.interieur.gouv.fr.

government; it participates in the defence of the fundamental interests of the state' (Decree 85-1057, 2 October 1985). Notably, these interests are further defined in the French Penal Code (section 410-1) so as to include France's independence, the integrity of its territory, its security, the republican form of its institutions, its means of defence and of diplomacy, the protection of its nationals in France as well as in foreign countries, the environment, essential elements of the country's scientific and economic potential, and its cultural heritage (Brodeur and Dupeyron, 2003, p. 15). Quite rightly, Brodeur and Dupeyron maintain that:

> inasmuch as the DCRG informs the French government on all topics relevant to its fundamental interests… there is in fact no sphere of activity that could possibly be excluded from its intelligence gathering mission (Brodeur and Dupeyron, 2003, p. 15).

Not surprisingly, the DCRG keeps hundreds of thousands of dossiers on individual French citizens (Porch, 1995, p. 423), which is why the DCRG enjoys the poorest reputation of all intelligence services in terms of public opinion (Brodeur and Dupeyron, 2003, p. 16). It has also carried out secret polls for the Ministry of Interior which the government has traditionally relied on in the preparation of public broadcasts on contemporary issues. 'The major complaint about this area of DCRG activity is that its research is initiated and pressed into the services of the party in power' (Brodeur and Dupeyron, 2003, p. 424).

Both French foreign and military intelligence services are formally under the authority of the MoD. With regard to external security services, the *Direction Générale de la Sécurité Extérieure* (DGSE) gathers and exploits intelligence with a bearing on France's security and detection of activity outside the country directed against French interests. Subordinate to the MoD, the DGSE replaced the controversial *Service de Documentation Exterieure et de Contre-espionage* (SDECE) in 1982. The DGSE, unlike the SDECE, is not permitted to operate on French soil. Douglas Porch emphasises the military nature of the French foreign intelligence, yet this has been gradually changing as civilians replaced the top military management of the DGSE over the last two decades (Porch, 1995, p. 469).

With regard to military intelligence, the *Direction du Renseignement Militaire* (DRM) ranks among France's most recent additions to the national intelligence sector. The initial reasons for the creation of a new type of military intelligence service came from the desire to overcome shortcomings observed during the Gulf War. Hence, the DRM's founding decree of June 1992 tasks the directorate with planning, coordinating, and leading investigations and the use of military intelligence. Yet, over time the DRM's responsibilities have gradually evolved from purely military intelligence to intelligence of military interest, and finally to the political and strategic intelligence that is the primary responsibility of the DGSE.[9] From the perspective of civil-military relations, the DRM is not an agency responsible for internal security, that is, its employees are not spies but soldiers. Yet the DRM Director reports directly to the Defence Ministry, rather

9. Available at: http://www.globalsecurity.org/intell/world/france/drm.htm.

than through the armed forces chiefs of staff to whom the Directorate is attached (Federation of American Scientists, 1997).

The *Direction de la Protection et de la Sécurité de la Défense* (DPSD) is also under the direction of the French Defence Ministry. Responsible for military counter-intelligence operations and the political surveillance of the military, its main task is to ensure the political reliability of the armed forces and other military security duties.

Lastly, the Office of the Prime Minister has three main intelligence institutions under its supervision. This concerns the *Secrétariat Général de la Défense Nationale* (SGDN), the *Direction Centrale de la Sécurité des Systèmes d'Information* (DCSSI) as well as the *Comité Interministériel de Renseignement* (CIR). Whereas the SGDN, unofficially referred to as the 'Prime Minister's Intelligence Service' has a mandate that resembles the DCRG's brief, the DCSSI serves as the body to protect government files and data (Henderson, 2002, p. 53). The CIR takes on the difficult role of coordinating the French intelligence community. The Committee is chaired by the Prime Minister and meets approximately twice a year to discuss pressing issues on the nation's intelligence agenda. The table below provides a rough overview of the main French intelligence services addressed in this article.[10]

10. Table 8.1 does not pretend to be exhaustive, but includes the major services. Services which are not included are, among others, BRGE (Intelligence and Electronic Warfare Brigade), the DCPJ (Judicial Police), CRS (Companies for Republican Security), CNCIS (National Commission for the Control of Security Interceptions).

**Table 8.1 Overview of Selected French Intelligence Services**

| Agency | Legal basis | Mandate | Accountability Provision | Budget (Year) | Staff |
|---|---|---|---|---|---|
| DST | Decree # 82–1100 (December 1982) | Internal counterespionage, anti-terrorism, espionage in economic, scientific and technical domains | Placed under the MoI, it answers to the Prime Minister's Office | ~73 Million USD (1995) | 1, 500 |
| DCRG | Decree # 85–1057 (October 1985) | Collection and centralisation of intelligence for the government incl. intelligence on political and labour upheavals | Placed under the MoI, it is responsible to the National Police (DGPN) | n/a | ~3, 200 |
| DGSE | Decree # 82–306 (April 1982) | Foreign intelligence collection, Counter-espionage | Placed under the MoD, it answers to the Prime Minister's Office | 310 Million USD (2000) | 4,100 |
| DRM | Decree # 92–523 (June 1992) | Military intelligence collection and assessment | Reports directly to the MoD | 12.5 Million USD (2000) | ~1, 700 |
| DPSD | Decree # 81–1041 (Nov 1981) | Responsible for protection and security of defence personnel and facilities | Subordinate to the Defence Staff which in turn reports to the Supreme Council of Defence | 9.5 Million USD (2000) | ~1, 600 |
| SGDN | Decree # 78–78 (January 1978) | Research and centralisation of intelligence for the government | Placed under the Prime Minister's Office | n/a | ~3, 200 |
| DCSSI | Decree # 2001–693 (July 2001) | Protection of government data and information systems, cryptography | Under the Prime Minister's Office | n/a | ~100 |
| CIR | Decree # 89–258 (April 1989) | Coordination of the national intelligence community | Reports to the Prime Minister | n/a | n/a |

*Source*: Henderson, 2002, pp. 51–54; Brodeur and Dupeyron, 2003, pp. 14–18

*Civil Management and Oversight Bodies*

Both the legislature and the executive play important albeit distinct roles in the governance of the intelligence sector. In liberal democracies it ought to be the legislature (and thus the elected representatives of the French voters) which provides the legal framework for the services. Rather than through government decrees, this should be done by adopting intelligence legislation in parliament. As previously indicated, each French intelligence service has been created with the help of a governmental decree (Brodeur and Dupeyron, 2003, p. 14). Thus the rules for intelligence services were not openly discussed in the plenary but decided upon by a very small circle of politicians and officials. While legislatures can also review the intelligence services' use of their powers and their expenditures, it is for practical reasons and because of the sensitive nature of the subject matter that effective external control and judicial review of the intelligence agencies is allotted to the government and the judiciary (Born and Leigh, 2005, p. 55). More concretely, the executive is responsible for the day-to-day management of the services. It tasks and prioritises the services and ensures that they stay out of the political process. What is more, it ensures that the intelligence services take the initiative whenever necessary, cooperate with other agencies, respect human-rights and abide by the rule of law (Maria de Puig, 2005). Arguably, executive control and parliamentary oversight constitute each other: 'parliament can only reliably call Ministers to account for the actions of intelligence agencies if Ministers have real powers to control and adequate information about the actions taken in their name' (Born and Leigh, 2005, p. 55). Likewise, the quality of executive control depends on the degree to which parliaments are enabled and motivated to perform their respective oversight tasks. Comparative research on parliamentary oversight committees has shown that significant differences exist with regard to the independence of parliamentary intelligence oversight committees *vis-à-vis* the executive, the degree of access to classified documents granted to the oversight committees, and the ability of the committees to maintain secrets. Furthermore, parliamentarians were especially keen to be involved in ad hoc inquiry commissions, for example after press leaks or intelligence scandals. Understandably, most Members of Parliament (MPs) like to perform in ad hoc inquiry commission as it guarantees, among other things, substantial media attention. Yet what is much more important, but less popular, are routine, ongoing intelligence oversight tasks where MPs in intelligence oversight committees perform frequent inspections and other unglamorous jobs (Born, Johnson, and Leigh, 2005, p. 238).

In terms of executive intelligence control in France, the presidential *domaine reservé* is substantial. The 1958 Constitution enshrines the President as guarantor of national independence and the integrity of the territory. It names the President as the commander of the armed forces and leader of the higher councils and committees of defence. Although most of the national intelligence services are subordinated to the MoD, by decree the agency heads are responsible to the President and the Prime Minister, not to the MoD. Apart from the individual

competencies of the French President, the Prime Minister and the Heads of several ministries, executive control over the intelligence and security services rests with two institutions: the *Conseil de Sécurité Intérieure* (CSI) and the *Comité Interministériel du Renseignement* (CIR), the latter being subordinate to the *Secrétariat Général de la Défense Nationale* (SGDN). The CSI, in its current form, is a novel institution in French politics. Created by decree just after the French presidential elections in May 2002, the CSI is directed by the French President, not the Prime Minister. Next to the President, the CSI includes the Prime Minister, the Interior Minister and the Ministers for Justice, Defence, Finance, Budget and Overseas as well as the CSI General Secretary. The General Secretary, nominated by the President, convenes and manages (in liaison with the SGDN) the confidential meetings of the council. The CSI's primary goal is to coordinate domestic security and to evaluate and to control the implementation of decisions by the services (Faupin, 2002, p. 5). By contrast, the CIR is more of a clearinghouse of French intelligence that prepares consolidated intelligence for the government. It is led by the French Prime Minister and gathers experts of different ministerial agencies united in the task to coordinate and supervise the services. The fact that the two prominent *fora* of civil management of the French intelligence services are no longer presided over by the same person, indicates a laudable step towards more multiple advocacy.[11] Due to the absence of multiple advocacy in the past, political leaders' personal biases had greater impact on the decision-making (be it because they claimed to know all the facts themselves or because they have already committed their administration to a particular course of action). It is therefore encouraging to see how the new system facilitates openness to decision-making alternatives by placing two different individuals at the apex of the two *fora* entrusted with civilian management of the services. Despite this, executive control over the country's intelligence services remains underdeveloped. The French executive, at least by European comparison, maintains an insufficient interface between the country's intelligence services and the state. This has often been lamented by French intelligence officials arguing that the present system lacks a pro-active management scheme that imposes clear and transparent communication and planning for both sides involved.[12] In this regard, one can point to several ways of avoiding ministerial abuse of the services. First, one can reasonably expect from the executive to submit its tasking directives to the services in writing.[13] This rule coupled with the requirement that such communication will be archived and copied to an independent oversight institution (for example, the Inspector-General) seems laudable inasmuch as it can help to deter illicit practices.[14] What is more it avoids

11. Multiple-advocacy, demanding that any decision-making process should be structured in a way so as to ensure that all viewpoints on an issue are given to the decision-maker before a decision is made. Bose, 1998, p. 124.
12. Based on communication between authors and French intelligence experts, Autumn 2005.
13. This requirement has been added to the Hungarian intelligence law; see the Hungarian Act on the National Security Services 1995, section 11.
14. Further means to avoid ministerial abuse are listed in: Born and Leigh, 2005.

the awkward conundrum over who gave what order to whom at what moment that has characterised the (limited) investigation into the Rainbow Warrior scandal (see below).

Speaking about parliamentary oversight, it is not envisioned that the legislature should interfere with the conduct of ongoing intelligence operations. This could draw intelligence services into political controversy and ought to be prohibited. Of all western democracies, France is furthest away from such poor practice. Yet the French National Assembly and the French Senate face an even graver problem: they have practically no say on intelligence control matters. Indeed, this has, at different moments in time, been much deplored by French parliamentarians and the general public at large, for example, in 1986, when despite public demand, no parliamentary inquiry examined the erroneous relationship between the executive and the services following the Rainbow Warrior affair; and in the late 1990s when both the Senate and the National Assembly produced two propositions in view of establishing two separate parliamentary intelligence oversight committees in each house (*Le Sénat*, 1999; *L'Assemblée Nationale*, 1999). Regardless of these efforts, in 2005, France still does not have her own parliamentary committee to scrutinise both her intelligence services and their management by the executive. This is deplorable for many reasons: first, France stands isolated among western democracies and can hardly function as a role model with regard to reform efforts of EU and CoE member states. Second, and more important for French politics, is the fact that it is in specialised parliamentary committees where 'effective scrutiny of security [through] painstaking and unglamorous work' is conducted (Born and Leigh, 2005, p. 77). Such committees are firmly established parliamentary practice in other democracies, where they review the legality and the effectiveness of the services. To this end, parliamentary committees can scrutinise (at times even authorise) the budget for intelligence services, produce annual reports to parliament, perform separate investigations (sometimes endowed with subpoena powers), and may even request prior notification from the services about future operations. In France no such oversight exists, intelligence chiefs and ministerial heads have never appeared before parliamentary committees and the budget of the services form a great part of the *fonds spéciaux*, which are not subject to review by the otherwise powerful French parliamentary finance committee.

Any reform proposal intended to modify this outdated practice faces stiff resistance, interestingly not only from the services but also from parliamentarians. When asked about recent reform propositions, the former head of a French intelligence service stated that '*il est inconcevable que des parlementaires puissent avoir un droit de regard sur l'utilisation des fonds secrets*' (it is inconceivable to grant parliamentarians a right to know how the secret budget is being spent). To him this is justifiable because '*demander à des législateurs de couvrir de facto des actes parfois illégaux n'est pas dans la culture française*' (to ask legislators to *de facto* conceal actions that at times have been illegal is not part of the French culture) (Roussin, 1999). Given that parliamentarians are elected representatives of the people, former French Defence Minister Paul Quiles rightly points to the weak

foundation of this position: how can one expect parliamentarians to content themselves with voting on a budget without knowing its utilisation (Quiles, 2000, p. 49)? As previously indicated, even among French legislators one finds scepticism if not outright opposition to the idea of a French parliamentary intelligence oversight committee. The former chairman of the Senate's Defence and Foreign Affairs Committee, Jean Lecanuet 'denounced public oversight of the secret services through parliament as nonsense. Parliamentary control is too dangerous' (Porch, 1995, p. 466). Douglas Porch gives an important insight as to why there is notable resistance even from the ranks of the main beneficiaries of such a reform project: substantial numbers of French parliamentarians simply do not see the personal benefits from such an engagement. 'French politicians have concluded that secret services bring them no votes when things go right and only headaches when there is a *bavure*, a mistake' (Porch, 1995, p. 466). We note that the French parliament has very little impact on the governance of French intelligence.

An important additional control body exists in the form of the main data protection authority in France, the *Commission nationale de l'informatique et des libertés* (CNIL). It is an independent agency which enforces the French Data Protection Act of 1978. This act deals with personal information held by government agencies and stipulates that anyone wishing to process data must register and obtain permission to do so from the CNIL. In addition, it provides that individuals must be informed of the reasons for collection of information and may object to its processing either before or after it is collected. It grants individuals the right to access information being kept about them as well as the right to demand the correction or deletion of erroneous data.[15] However, together with other EU members, France should have amended its data protection regime to make it compatible with the European Union Data Protection Directive (95/46/EC) by 1998 (Privacy International, 2003). Unfortunately this process has not yet been finalised and it remains to be seen whether CNIL will extend its remit to the data collection of the French intelligence and security services. At present the chances are slight, because the National Assembly, following a government proposition, has decided that the reform of the 1978 Data Protection Act should not apply to the treatment of data that concerns national security, that is, the data kept under the direction of the DST or DGSE (*Commission nationale de l'informatique et des libertés* (CNIL), 2004). At present, CNIL aims to downplay the effect of this decision by saying it bears neither an effect on the right of CNIL to publish an official opinion on the handling of data which concerns national security nor on its right to indirect access to the contested files by those members of the CNIL who serve as magistrates. At any rate, this falls far short of an official remit over the data held by the security services and thus offers little public control.

15. Law No. 78–17 relating to data processing, files and freedoms, available at: http://www.cnil.fr.

*Justice and Law Enforcement Institutions*

By international comparison, the French legal institutions, especially the French investigating magistrates, play a much more visible role in the national intelligence sector. A priori, the role of the courts of law in the intelligence sector includes the important task of judging whether the intelligence services have received sufficient authorisation for the usage of their exceptional powers (for instance, wire-tapping, surveillance, interrogation practices, data collection, and so on). Furthermore, most judgements are given after the fact, that is, courts have the jurisdiction to determine whether operations that citizens or intelligence staffers have brought to their attention are within the law. If the courts find that an action of the intelligence and security services has unjustly violated a person's rights, they can decide on appropriate compensation for the affected individual or organisation (Maria de Puig, 2005, para. 44). One of the institutions that spring to mind in this regard is the *Conseil d'Etat*, which combines the functions of the highest administrative court with that of a government consultancy. Similarly to what justice ministries do in other democracies, the *Conseil d'Etat* examines the legality of laws before presenting them to the Council of Ministers. For our review of the French intelligence governance it is noteworthy that the *Conseil d'Etat* produced new jurisprudence on the right of individuals to access personal files kept by the intelligence services. In July 2003, the *Conseil d'Etat* ordered the DCRG to inform Michel Raoust (President of the French Committee of Scientologists Against Discrimination) about personal data they hold about him. Prior to this ruling, the DCRG had successfully argued before lower courts that 'public security' outweighs Mr. Raoust's right to information. Not disputing that this might be true in some circumstances, the *Conseil d'Etat* specified that 'public security' must not remain a motive of general character if it is to be accepted by the court. There need to be 'elements' in the argumentation that enable the jurists to decide whether the intelligence services are correct in assuming that personal information cannot be granted without undermining public security (Human Rights Without Frontiers, 2003). In this manner, the judgement speaks of a successful judicial review upon the practices of the intelligence services.

A second important judicial institution in the French intelligence sector is located within the Trial Court of Paris. In France, any prosecutor can take a decision whether a crime committed within his geographic area of responsibility is related to terrorism, based on a definition of terrorism as 'acts committed by individuals or groups that have as a goal to gravely trouble public order by intimidation or terror' (Shapiro and Suzan, 2003, p. 77). Should the act before the prosecutor merit this definition, the case is then referred to specialised prosecutors or magistrates within the Paris court (Shapiro and Suzan, 2003, p. 77). Interestingly, the investigating magistrate is not an advocate for the prosecution or the defence, but someone tasked to conduct an impartial investigation that determines whether a crime worthy of prosecution has been committed. Since they are intended to be impartial arbiters, they are granted a wide array of competencies for their investigations without having to answer to any political authority. This

unique judicial task force has received international media interest not only because of the splendid reputation it enjoys for its alleged capability to apprehend suspected terrorists but also for its unique competencies. The German weekly *Die Zeit* depicts the special Trial Court of Paris as:

> [A] singular authority which unites powers of the secret service, public prosecution, the legal system and the police, which far exceeds the limits of the division of power. They can order the shadowing of suspects, searches, wire-tapping, and possess subpoena and arresting powers and can impose sentences (Mönninger, 2004).

The investigating magistrates gradually accrued more and more competencies over time and developed formidable expertise on the subject matter through years of investigations. In 1996 an important legislative reform was introduced with Article 421-2-1 of the French Penal Code. It made the conspiracy to commit terrorism as grave an offence as an actual act of terrorism. In so doing, the French magistrates working on these cases were empowered to open 'investigations and to deploy their expertise and judicial tools before terrorist attacks took place, thereby enhancing their competences not just for punishing a terrorist act but also for preventing them in the first place' (Shapiro and Suzan, 2003, p. 82). The growing expertise among the investigating magistrates inspired the DST agents:

> … to now go directly to the magistrate when they have information that they feel warrants a judicial investigation. While information before a judicial investigation is opened is not admissible before French courts, the opening of an official investigation provides various advantages because the agents in question can from that point onward avail themselves of the magistrates' extensive powers to issue warrants, subpoenas, wiretaps, the results of which can be used in court (Shapiro and Suzan, 2003, p. 83).

Although effective, the special relationship between the intelligence and security services that has become common practice in France needs critical counsel from the angle of good governance.

## The Quality of Governance Over the French Intelligence Sector Assessed

The remaining part of the chapter assesses holistically the quality of governance over the French intelligence sector. In so doing, the text does not account for the increasing scale of French engagement in European and international intelligence cooperation. Although very important, this theme involves a wide circle of French and international actors that go much beyond the scope of the already complex nature of the French intelligence sector, the primary focus of this analysis.[16]

16. See further: Gregory, 2003, pp. 123–147; US Department of State, 2005, pp. 46 ff.; Shapiro and Suzan, 2003; Priest, 2005; Daun, 2005, pp. 135–149; Assembly of the Western European Union, 2002.

The number of political scandals involving the executive and the intelligence services give evidence of poor democratic intelligence governance in France. Arguably, the practice of co-habitation in government coalitions and the inherent rivalry between a socialist President and conservative PM in the 1980s and 1990s has done little to ensure objective executive control. Many scandals point to practices in which French politicians have used the intelligence services to their own personal ends. The most prominent intelligence disaster is the Rainbow Warrior affair. In Auckland harbour, on the night of 10 July 1985, as 'the fruit of a long-term contingency plan' (Porch, 1995, p. 457), two DGSE agents placed a bomb on the Greenpeace ship Rainbow Warrior, which killed one photographer and caused the ship to sink. The Rainbow Warrior was used in order to protest and, if possible, to prevent French nuclear testing on the nearby Moruroa atoll. The covert operation was quickly uncovered and laid bare a highly problematic relationship between the intelligence services and the government.[17] The interesting aspect of this scandal is not so much the weak performance of the services[18] but the way in which the executive has most likely put in practice the plausible deniability principle. Plausible deniability depicts a political doctrine which involves the creation of power structures and chains of commands loose and informal enough to be denied by the political administration if necessary.[19] With regard to the Rainbow Warrior affair, the then French President François Mitterrand and his Ministers have consistently denied any knowledge of 'Operation Satanic'. Mitterrand sharply criticised the 'rogue agents' and ordered an investigation to find out the truth about this scandal which damaged the French relations with Australia and New Zealand. The inquiry exonerated the French cabinet but led Mitterrand to dismiss both the Defence Minister and the head of the DGSE, Admiral Lacoste. In 2005, new information came to light which reinforced wide-spread speculations that the French President himself ordered the bombing of the Greenpeace vessel (*The Times*, 11 July 2005). Admiral Lacoste now reports that after the French Defence Minister had assigned a sufficient amount of money from the secret funds for 'Operation Satanic', he then assigned the DGSE chief, to 'neutralise the Rainbow Warrior'. Admiral Lacoste sought confirmation from President Mitterrand who is said to have given his agreement by stressing the importance that he attached to the nuclear tests (*The Times*, 11 July 2005).

Another reported incident can be listed *vis-à-vis* the possible use of the plausible deniability doctrine. In July 2002, the French daily *Le Monde* reported that President Chirac had sacked the DGSE head, Mr. Cousseran for having allowed investigations into alleged links between Lebanese Prime Minister Rafiq Hariri and former Japanese financier Shoichi Osada (*Le Monde*, 2002). Chirac

17. For an excellent account on *l'affaire Rainbow Warrior*, Porch, 1995, pp. 455–468.
18. According to one commentator, 'so clumsy was the operation, so indiscreet the agents, so obvious the trail of evidence that the agents might as well have left a beret, a baguette and a bottle of Beaujolais at the scene of the crime', Dyson, 1986, p. 95.
19. Born and Leigh, 2005, p. 65. A more detailed review on the 'sociology of denial' as it pertains to global human rights protection during the 'war on terror' is given by Welch, 2003, pp. 1–20.

argued that the investigations revived old unfounded rumours that a covert ransom was paid to the government of Iran for releasing French hostages in 1988. Official government spokesmen have always denied that any such payment was made. Despite these denials, the *Le Monde* article spurred a renewed debate in French politics as many believe that a substantial amount of that ransom money had been pocketed by French politicians, including Mr. Chirac, who was France's Prime Minister at that time. Whatever the real involvement of the French President, a more effective executive control of the intelligence services characterised by multiple advocacy would have probably prevented the implementation of the 'lunatic order' that led to the Rainbow Warrior affair (Porch, 1995, p. 459). Having said this, an even more useful and legitimate tool to prevent such scandals can be seen in an effective system of checks and balances between a strong executive and a strong parliament. This would have moderated the obstructive executive dominance in decision-making before and after the scandal. Yet, the resistance to a parliamentary inquiry in the aftermath of this affair must also be mentioned, even though it serves as a reminder of the immaturity of intelligence governance at that time.

Another important scandal, often dubbed the French 'Watergate' (*Associated Press*, 2004), should also be included here. It was only in November 2004 that twelve former government officials and senior police officers went on trial charged with running a phone-tapping operation used by Mitterrand to keep tabs on his personal enemies. The scandal emerged after transcripts were leaked to the Paris daily *La Libération*, showing that a special counter-intelligence group directly responsible to President Mitterrand illegally wire-tapped numerous people during the 1980s. Conceived in 1982 as a special antiterrorist unit that answered to the President, the team ended up eavesdropping on journalists, lawyers and businessmen in a bid to discover embarrassing information and potential scandals. Yves Bonnet, head of the DST intelligence service at the time, told the *Le Parisien* newspaper that the wiretaps the Elysée asked for never served the struggle against terrorism. Notably, although the scandal broke out in 1992, it took until 2004 to open the trial. This has to do with the wide powers of France's presidency and the secretive ways of its judicial system. It was not until 1998 that the Socialist Prime Minister, Lionel Jospin, waived the official secrets act in the case to require officials to divulge information they had kept quiet. Unlike President Nixon in the Watergate scandal, President Mitterrand was never held accountable for this prime example of poor governance.

Albeit of primary importance, the French executive is not solely responsible for instances of poor practice. Weak spots can be identified also with the intelligence services, the parliamentarians' resistance to the creation of intelligence oversight structures, the judiciary and civil society at large. With regard to the intelligence services, history is full of examples where political leaders have influenced intelligence services more than the intelligence services were able to influence the decision-making of political leaders. Evidently, this creates power struggles among the national intelligence services in terms of public funding and general reputation. The best example is that the French DST supported the New

Zealand police in its investigation of the Rainbow Warrior scandal, which greatly infuriated the French DGSE (Porch, 1995, p. 464).

Large bureaucracies such as intelligence services create over time mechanisms to defend and perpetuate their own interests and power. This bears the negative connotation that few intelligence staffers are willing to put forward information that conflicts with a leader's preconceptions as this might thwart their chances of obtaining executive support. In this regard both the gradual development towards the creation of multiple advocacy in the CSI and CIR are welcomed as steps in the right direction. Of course this ought not to be confused with democratic intelligence governance introduced in the second section of this article. What is more, it seems plausible that the increasing importance of the French investigating judges has depoliticised intelligence governance at least with regard to international terrorism. 'As specialised investigating magistrates became more publicly visible, they achieved a greater capacity to assert their statutory independence from political authorities' (Shapiro and Suzan, 2003, p. 78). Perhaps the growing success and public confidence of the French in the magistrates have been greeted by politicians with relief as it spared them from some of the political responsibility over the security services.

The chapter has already pronounced upon the negative consequences that accrue from the lack of parliamentary intelligence oversight in France. To have no parliamentary intelligence oversight committee that examines the effectiveness and the legality of the services remains the single most obvious deficiency of the French intelligence sector. As the continuing resistance by parliamentarians to the creation of such institutions in the Senate and the National Assembly demonstrates, this has much to do with the '*handicaps culturels de la France*' that is, the lack of an intelligence and accountability culture among politicians and citizens alike. This summarises the position of Senator About, who regrets the fact that the intelligence services are suspicious and often discredited in the eyes of the French. He blames the general attitude of Frenchmen of being wary of authority and willing to circumvent the law wherever possible. Senator About also disapproves of the conduct of French politicians who consider intelligence as a matter of high politics, which concerns specialist but certainly not French citizens (Le Sénat, 1999).

Related to the absence of parliamentary involvement, as mentioned before (see Table 8.1), all French intelligence and security services are functioning on the basis of an executive decree instead of a statutory law enacted by parliament. From the standpoint of democratic governance, this is problematic for at least two reasons. Firstly, an executive decree pre-empts parliament from having a say about the contents of the legal framework of the services, which usually includes the services' mandate, powers, accountability and reporting mechanisms, budgetary controls, as well as practical and coordinating provisions concerning the work of the services. Cutting parliament out of intelligence legislation seriously impairs the system of checks and balances and blocks substantial debate in parliament about the direction and position of the services in French society. Parliamentary debate alone can provide democratic legitimacy to intelligence legislation. Secondly, according to Article 8.2 of the ECHR, any interference with private communication

and property by a public authority (for example, internal security services) has to be 'in accordance with the law'. Though the European Court in Strasbourg has in some instances disqualified a decree for having insufficient legal basis for the interference of privacy by internal security services, it has not categorically ruled out a decree as a legal foundation for internal security services. Nevertheless, case law of the European Court in Strasbourg has spurred various governments of states in Europe to legislate properly their internal security services (for instance, in the United Kingdom and the Netherlands) (Cameron, 2000, sections 1.4.4, 2.6 and 3.4). Additionally, the European Commission for Democracy Through Law (the 'Venice Commission'), the Council of Europe's top advisory body on constitutional issues, has expressed that legislation is to be preferred above government decrees (Venice Commission, 1998).

Fortunately, the authors can also report on two recent developments that denote a more active involvement by parliamentarians in the French intelligence sector. First, on 24 November 2005, the National Assembly has amended the government's new anti-terrorist bill by adding a surprise proposition that called for the creation of a parliamentary intelligence oversight committee. What brings new momentum to this six year old debate is that the French Interior Minister, as well as the majority of the country's parliamentarians, have expressed their support for this initiative (*Le Figaro*, 25 November 2005; *Le Monde*, 29 November 2005). The National Assembly adopted the amended anti-terrorist bill on 29 November 2005. Thus at last, France seems prepared to provide for more rigorous parliamentary intelligence oversight. In his speech before the National Assembly, Interior Minister Nicolas Sarkozy promised to establish a study group of parliamentarians and representatives of the intelligence services that will, by February 2006, have evaluated the modalities for the creation of a parliamentary intelligence oversight commission. Interestingly, the Interior Minister assured the French Assembly that the heads of the French security services are in favour of institutionalising parliamentary control of the intelligence services.

Second, up until 2002, the utilisation of the '*fonds spéciaux*' (a great part of which is allotted to the funding of the intelligence services) has been withheld from parliamentarians' eyes. The review was done by a special verification committee, nominated by the French President and which consisted of the following persons: it was led by a President of one of the French audit court's chambers, and included two commissioners chosen among the members of the Council of State, Audit Court or the general finance inspection office. This changed with the introduction of a new financial law in 2002, which altered the constitutional set-up of the verification committee. It now comprises two National Assembly deputies (appointed by the President of the National Assembly) and two senators (appointed by the Senate's President) and two members of the audit court (appointed by the President of the audit court). This denotes an important leap forward towards parliamentary control of the services' expenditures. The verification commission is now granted access to all documents which enables it to form a realistic picture of the incurred costs paid by the *fonds spéciaux*. Furthermore, the verification committee drafts a report which it gives to the French President, the Prime Minister

and to the Presidents of the finance committees of the Senate and the National Assembly. It also has the power to hold hearings aiming to establish whether the incurred costs are justified by the documents presented to it. Similar to parliamentary practice in most other nations, the verification committee has no remit over ongoing intelligence operations (Le Sénat, 2003). This notable progress notwithstanding, it must also be stated that the verification commission is still reactive in character and deals exclusively with financial aspects of intelligence services. What is more, the committee is not entirely 'owned by parliament' in the sense that it does not deal with the confirmation of top appointments or the effectiveness of the intelligence services.

## Conclusion

The system of checks and balances, originally devised by the great French philosopher Montesquieu, is, at best, insufficiently applied in France when it comes to present-day governance of the French intelligence services. The main point of critique lies in the fact that intelligence governance in France is still characterised by a dominant executive and a compliant parliament. Executive dominance can lead, and has led, to the politicisation of intelligence. It occurs especially when information from the intelligence services or the services themselves are used for personal or political purposes. The fact that this has not been a theoretical concern has been demonstrated by the limited selection of French intelligence scandals accounted for in this text. Experiences with parliamentary intelligence oversight in other democracies demonstrate that a more effective system of checks and balances, and in particular a much stronger countervailing parliament can make a tremendous difference in preventing the executive from using the intelligence services for personal use or in a manner that is beyond the law.

Having said this, it is also true that the French public, and French parliamentarians in particular, have not been very vocal in their request for a change in the system. Should there be greater parliamentary empowerment in intelligence affairs, MPs and the general public would need to express this desire more forcefully. In this regard it is unfortunate that on 23 November 1999, the Defence Committee of the French National Assembly examined the detailed proposition on the creation of a Parliamentary Intelligence Oversight Commission without taking any further steps. In the end, the National Assembly did not endorse the proposition which leads to the question: how prepared is the French political culture to embrace the concept of a democratically governed intelligence sector?

Chapter 9

# Parliamentary Oversight of the Norwegian Secret and Intelligence Services

*Ambassador Leif Mevik and Hakon Huus-Hansen*

## Introduction[1]

In Norway, oversight of the secret services is carried out by a parliamentary body, the Committee for the Monitoring of Intelligence, Surveillance and Security Services.[2] The Committee conducts constant monitoring of the Norwegian Police Security Service, the Norwegian Intelligence Service and the Norwegian National Security Authority (in Norwegian shortened to the 'EOS services'). This arrangement is independent of both the EOS services and the remainder of the public administration. The Committee's members are elected by, but are not themselves members of, the *Storting* (the Norwegian parliament). The Committee was established in 1996 by Act of Parliament and it reports to the *Storting* annually. Oversight is assured through regular inspections of the secret services. The Committee also deals with complaints from private individuals and organisations who believe the secret services have committed injustices against them.

The objective of this article is to give an overview of the Norwegian oversight system. After an account of the historical background of the present system, the statutory framework is described, followed by a discussion of the various monitoring activities.[3]

---

1. The term 'monitoring' is used here as an alternative to the translation 'oversight' to render the gambit of activities exercised by the Committee for the Oversight of Intelligence, Surveillance and Security Services. This is not an incidental difference but signifies a greater attention to detail in their overseeing of intelligence activities than is the norm in other comparable oversight systems. Both oversight and monitoring are distinct from the surveillance practices of the intelligence services being audited.
2. The website of the parliamentary oversight committee is: http://www.eos-utvalget.no/.
3. It must be underlined that this chapter is based on an insider's view. Between 1999 and 2006, the first author was chair of the Norwegian parliamentary body for the monitoring of intelligence, surveillance and security (EOS) services. The second author was Head of the Secretariat of the aforementioned body. An outsider's account can be found in Sejersted 'Intelligence and Accountability in a State without Enemies: The Case of Norway' in Born, Leigh and Johnson, 2005.

**Background for the Current National Intelligence Monitoring System**

As in many other western countries, the end of the Cold War created a climate for debate in Norway about the secret services as well as a readiness for somewhat greater openness. During the 1970s and 1980s, the individual services, particularly the Norwegian Police Security Service, were also occasionally the subject of public debate, and received a certain amount of criticism on particular matters. In that era, radical movements on the political left wing experienced or maintained that they were subjected to a zealous and, in their view, groundless surveillance of their legitimate political activities. In these isolated cases, the public authorities never confirmed that the services had carried out activities of the kind their critics accused them of, and were certainly unwilling to admit that anything irregular had occurred. Criticism therefore often stagnated despite varying degrees of documentary evidence that something unlawful had taken place. These isolated cases gradually increased the suspicion among the general public that the secret services carried out political surveillance contrary to their regulations and official statements. However, it was not until after the fall of the Berlin Wall, when the traditional concept of the enemy had faded, that it became politically possible to have a more open and meaningful debate about the activities of the secret services and to put forward the idea of an independent inquiry into the services.

Partly as a result of the general public debate at the time, the *Storting* decided on 18 June 1993 to establish a parliamentary monitoring arrangement to strengthen oversight of the secret services. The government was given the responsibility, in consultation with the Presidium of the *Storting*, of appointing a commission to prepare a proposal for a monitoring model. This commission submitted its recommendations on 7 February 1994. At approximately the same time, on 1 February 1994, the *Storting* appointed a separate inquiry commission (the Lund Commission)[4] which was assigned the task of investigating the activities of the secret services during the period from 1945 until the date of the Commission's report. The work on a parliamentary monitoring arrangement resulted in Act No. 7 of 3 February 1995, which would regulate the Committee's activities. The first Committee for EOS Services was elected by the *Storting* and began its work in April 1996. Again, this was concurrent (this time deliberately) with the activities of the historical Lund Commission inquiry, which submitted its report to the *Storting* on 28 March 1996.[5] Thus, in two parallel chains of events, the *Storting* simultaneously provided for an independent inquiry into the historical activities of the secret services and, with a view to the future, the establishment of a parliamentary monitoring body with relatively wide-ranging authority. It may be said that the Lund Commission conducted a critical review of the past while the

4. The Commission was named after Ketil Lund, a judge of the Supreme Court of Norway.
5. This is the Lund Report, Document No. 15, (1995–1996).

Committee's responsibility involved (and continues to involve) helping to prevent the mistakes of the past from being repeated. The Committee's independence from parliament was deliberate, in order to avoid partisan considerations in the Committee's work – or accusations of such a nature.

The Lund Commission revealed that, well into the 1980s, the Norwegian Police Security Service had conducted relatively extensive unlawful registration and surveillance of political left wing persons and organisations. The Commission was also critical of aspects of the activities of the Norwegian Defence Security Staff in relation to the security clearance of persons. No major criticism was levelled against the Norwegian Intelligence Service. The Lund Commission's report was extensive and thorough and enjoyed general acceptance on both sides of the political landscape. Besides providing a broad account of the investigations that had been made including their factual circumstances, the commission reviewed the regulations for the services and considered many major legal issues. Here one might particularly mention the interpretation of the rules for registration in the archives of the security police, and for establishing more active person-oriented investigations. Thus, particularly during the years immediately following 1996, the Lund Report was an important reference for the work of the Committee for Monitoring of Intelligence, Surveillance and Security (EOS) Services.

The political climate in Norway in 1996 was, generally speaking, well disposed to improving the accountability of intelligence services. The Lund Report's exposure of grounds for criticism up to recent times contributed to this, and it was in this political and social context that the Committee for Monitoring of Intelligence, Surveillance and Security Services began its work. Naturally, there has since been a certain re-emphasis in the direction of what might be referred to as traditional political dividing lines regarding the need for effective secret services or, to put it more precisely, the balancing of monitoring activities in relation to this consideration. There is no doubt that monitoring can have a restrictive effect on the operations of the services and on their partners' trust in them. It is a question of where the point of balance should be placed. This affects both the formulation of monitoring regulations and the enforcement of the regulations. It is the Committee's experience that continuous work and awareness of the shifts in society's general attitude towards the services and their work, is essential here.

External monitoring of two of the secret services (the Norwegian Police Security Service and the Norwegian National Security Authority) was established as early as the early 1970s through a government-appointed supervisory committee consisting of three persons. This committee, which was subjected to a certain amount of criticism by the Lund Commission, was abolished when the Committee for Monitoring of Intelligence, Surveillance and Security Services was established. In the case of the Norwegian Intelligence Service, the latter Committee provided the first external monitoring of its activities.

## The Norwegian Framework for Intelligence Monitoring

### *The Mandate of the Monitoring Committee*

The Committee's activities are regulated by Act No. 7 of 3 February 1995 and by supplementary instructions issued by the *Storting* on 30 May 1995.[6] It is the Committee's responsibility to monitor the activities of the EOS services conducted in the interests of national security under the aegis of public authority. Intelligence, surveillance and security services that have purposes other than the protection of national security, for example ordinary criminal intelligence and traffic surveillance, are not included in the area of supervision.

The area to be monitored is functionally defined, and not associated with specific organisational entities. It is therefore not of decisive importance for the monitoring authority which body or agency performs EOS services at any given time. These duties are currently assigned to the Norwegian Police Security Service, the Norwegian National Security Authority and the Norwegian Intelligence Service and consequently, it is these services that the Committee continuous to monitor. However, the Committee may also conduct investigations in other parts of the public service if this is found to be appropriate for clarification of the facts of a case.[7] The purpose of oversight is primarily that of safeguarding the rights of individuals under the law.[8] Pursuant to this provision, the Committee shall establish whether any person is being subjected to unjust treatment and also ensure that the EOS services do not make use of more intrusive methods than are necessary under the circumstances. However, the provision also specifies that the Committee shall conduct general monitoring in order to ensure that the activities of the EOS services are kept within the rule of law.

The responsibility for monitoring does not embrace activities involving persons who are not resident in Norway or organisations that have no address in this country.[9] The provision also makes an exception for activities involving foreign citizens whose residence in Norway is associated with service for a foreign state. This exception is especially intended for diplomatic personnel. However, the Committee may monitor these areas too if special grounds so indicate.[10] Finally, we might mention here that both the Act relating to the Norwegian Intelligence Service and the Act relating to the Norwegian National Security Authority include provisions that the services shall facilitate monitoring by the Committee. This

6. The Instructions are complementary regulations given by the parliament in addition to the formal law.
7. Section 3.3, the Act on the Oversight of EOS Services.
8. This is stated in section 2 of the Act relating to the Oversight of the EOS Services.
9. See section 4 of the Oversight Instructions.
10. This is expressly stated in section 4 of the Oversight Instructions but, for that matter, already ensues from the powers granted to the Committee by section 3, third paragraph, of the Act relating to the Oversight of Intelligence, Surveillance and Security Services.

involves *inter alia* the obligation to have systematically arranged archives that can be subjected to genuine control.

*Election and Composition of the Committee*

The Committee has seven members including the chairman and vice-chairman. The members are elected by the *Storting* in plenary session on the recommendation of the *Storting's* Presidium. The term of office is normally five years, but members may be re-elected. Deputies are not elected. The Committee conducts its day-to-day work independently of the *Storting*, and members of the *Storting* are not permitted to be members of the Committee simultaneously. The *Storting* has emphasised that the Committee should have a broad composition, representing both political experience and experience in other areas of society. The Committee's administration consists of the Committee's chairman, two legal secretaries, and an office secretary. All members of the Committee and employees of the secretariat are cleared for the highest security classification in accordance with national and NATO regulations. There are no other defined or formal criteria for selecting the chairman or members; especially for the chairman, the presidium will look for a person with broad experience who enjoys the general confidence of the S*torting*.

*The Principle of Post-Facto Monitoring*

Pursuant to section 7 of the Instructions for Monitoring of Intelligence, Surveillance and Security Services, the Committee shall abide by the principle of post-facto monitoring. By this is meant a control placed on intelligence services subsequent to their actions in order to ensure that they have complied with the law, that correct procedures have been followed and that the interventions that have been made have not been disproportionate. However the principle does not apply unconditionally. The same provision states that the Committee may demand access to information on current matters and submit comments on them. This balance between post-facto monitoring and the right of initiative is also reflected in other statutory provisions. For example, the responsibilities given to the Monitoring Committee are broad and impose on the Committee a certain duty to investigate matters and circumstances that it finds relevant to its mandate, particularly those matters which have attracted public criticism. At the same time, it is emphasised that oversight should be arranged in such a way as to interfere as little as possible with the day-to-day activities of the services (section 4.2, Instructions).

The central consideration consists, on the one hand, of avoiding monitoring that appears anticipatory and thereby may steer concrete operational steps. On the other hand, monitoring on an exclusively post-facto basis runs the risk of investigations in an individual matter becoming so irrelevant as to loose all their force. For example, some cases in the counter-intelligence work of the Police Security Service may take several years to investigate. If monitoring were to be unconditionally post-facto in relation to individual cases, this might result in inappropriate adaptations by the services.

Achieving a balance between these considerations may be difficult at times, particularly in relation to Police Security Service matters. However, it has proved difficult to formulate more precise criteria than those currently provided by the Act and Instructions. In other words, discretion must be used in each case to discern whether or not the Committee is to carry out investigations in relation to a case in progress, and, if so, whether it shall content itself with only a briefing and refrain from expressing any view on issues which may arise in such ongoing matters. This means that, over time, situations are bound to arise where the Committee and services disagree. It is particularly important that the monitoring of cases in progress be conducted in a way that does not have a steering effect and that may not be perceived as having such an effect.

*Prohibition of Consultation*

The principle of post-facto monitoring may be viewed in connection with the fact that the services are expressly prohibited from using the Committee for consultations.[11] This prohibition has virtually the same purpose as the principle of post-facto monitoring – to avoid elements of steering being included in the monitoring. The monitoring activities of the Committee are, as is explained in more detail below, based on extensive inspection activities, which involve frequent and regular meetings with the services, for example, six meetings annually in the headquarters of the Police Security Service. These meetings are normally also attended by representatives of the leadership of the services. When the Act on EOS Services was being drafted, there was an awareness that such frequent meetings would result in familiarity between the services and the monitoring body. A certain degree of familiarity creates a basis for trust and confidence, and these are necessary conditions for effective continuous monitoring. However, there is again a need for balance, since monitoring should be independent and free of the constraints of personal relations.

The prohibition against consultation is directed towards the services. It helps to sharpen their awareness that the monitoring body cannot be saddled with the responsibility for day-to-day arrangements. Moreover, in its inspection activities, the Committee is very alert to the fact that this form of encumbrance would be harmful to monitoring objectives.

*Relationship to the Superior Prosecuting Authority*

The public prosecutors and the Director General of Public Prosecutions constitute the superior prosecuting authority and are exempt from monitoring by the Committee as is stated in the Act itself.[12] Of the three services monitored by the

11. Section 2, final paragraph, of the Act relating to the Monitoring of Intelligence, Surveillance and Security Services.
12. Section 1, second paragraph of the Act relating to the Monitoring of Intelligence, Surveillance and Security Services.

Committee, it is only the Police Security Service, as a police body, that has the authority to conduct criminal investigations, (see below). The provision is thus aimed at monitoring this Service.

A thorough understanding of the provision requires an awareness of the dual responsibilities of the Norwegian Police Security Service. The Service conducts both preventive investigations and criminal investigations based on suspicion of criminal acts. This distinction is essential. The preventive activities of the Police Security Service are not criminal investigations. They are conducted pursuant to the Police Act and instructions issued by the Ministry of Justice. In relation to these activities, the Police Security Service is subject to the authority of the Ministry of Justice. However, when the Police Security Service conducts criminal investigations, its activities are regulated by criminal procedure law, and here the Police Security Service is not subject to the authority of the Ministry but to that of the superior prosecuting authority. In its investigative activities, the Police Security Service, like other police units in Norway, has the right to make prosecutorial decisions, such as whether a person is to be charged, whether the use of coercive measures such as telephone control or surreptitious searches are to be requested and whether prosecution is to be recommended. The prosecuting authority thus assigned to the police is a subordinate prosecuting authority, and the Police Security Service can be instructed by the superior prosecuting authority. It may be added here for explanation that in Norway, as in the rest of Scandinavia, law enforcement and intelligence are not separated.

The prosecuting authority in Norway has traditionally held an independent status as a guarantee against political pressure on prosecutorial decisions. This is reflected in the fact that, pursuant to the current rules of criminal procedure, the superior prosecuting authority can only be instructed by the King in Council. The superior prosecuting authority is exempt from monitoring by the Committee because it would be regarded as a breach of a long and stable tradition in Norway if a politically elected monitoring body were assigned the authority to monitor the superior prosecuting authority. The reason why the subordinate prosecuting authority is not exempt from monitoring by the Committee is that it would be difficult to draw a line between the investigative and preventive activities of the Police Security Service. It is, for example, conceivable that inquiries concerning a person are first of a preventive nature but the inquiries may then give cause for suspecting criminal acts, which would result in the start of an investigation. If the investigation fails to reveal anything, the case may be dropped, but there may still be grounds for maintaining a preventive case. It would be extremely difficult for the Committee to conduct effective monitoring if only some of the circumstances or progress of a case could be examined. Another reason for allowing monitoring of subordinate prosecuting authorities is that consideration for the independence of the prosecuting authority does not make itself felt to the same extent when it comes to the monitoring of a subordinate prosecuting authority.

The Police Security Services' activities thus fall within the monitoring responsibility of the Committee, both in investigative and in preventive cases. However, because there may be extensive contact and cooperation between the responsible officer in the Police Security Service and the public prosecutor in cases

involving investigations, the demarcation of the Committee's monitoring responsibility in these cases could be difficult. Questions concerning this issue have occasionally arisen in connection with the monitoring of the Police Security Service. In two major cases dealt with by the Committee, the relationship to the superior prosecuting authority and demarcation of the area of supervision were major issues (see also the section concerning the Police Security Service).

*The Committee's Power and Monitoring Instruments*

The Committee may express its views to the services on matters or circumstances it examines as part of its monitoring activities, and provide recommendations or guidance to the services, for example that a case should be resumed or that a measure or practice should be discontinued. However, the Committee has no authority to issue instructions or make decisions concerning the services.[13] It was an obvious requirement when drafting the law that a monitoring body elected by the *Storting* should not be able to make binding decisions concerning the public administration. Any other solution would have been a breach of Norway's constitutional system. The arrangement of the monitoring committee is largely based on the Norwegian arrangement concerning the Parliamentary Ombudsman.[14]

The means available to the Committee for bringing about changes in the services lie in the Committee's reports to the *Storting* on monitoring activities. In its reports, the Committee can call attention to circumstances and issues in the services that it regards as being of current interest. This provides the *Storting* with a basis for assessing whether, for example, amendments should be made to practice or regulations. Among the instruments available to the Committee besides the right of inspection, which is discussed in a separate section below, the Committee has the right to summon employees of the EOS services and other parts of the public administration as well as private individuals for oral examination by the Committee.[15] Pursuant to the same provision, the Committee may also apply for a judicial recording of evidence. Employees of the ministries are exempt from section 5, again this is for constitutional reasons. The Committee also has the right to engage expert assistance in monitoring activities where this is viewed as appropriate.[16] This is practised to a certain extent in the areas of computing and telecommunications, particularly in connection with monitoring of the Norwegian Intelligence Service.

13. This ensues from section 2, final Paragraph, of the Act relating to the Monitoring of Intelligence, Surveillance and Security Services.
14. Section 7, second Paragraph, of the Monitoring Instructions, which refers to the principles of Act No. 8 of 22 June 1962 concerning the *Storting*'s Ombudsman for Public Administration.
15. Section 5 of the Act relating to the Monitoring of Intelligence, Surveillance and Security Services.
16. Section 10 of the Act relating to the Monitoring of Intelligence, Surveillance and Security Services.

*The Committee's Right of Inspection*

The Committee has a broad right of inspection of the public administration's archives and registers as well as a correspondingly broad right of access to the public administration's premises and installations of all kinds.[17] Here too exemptions are made for employees of the ministries.

A broad right of inspection is necessary in order to enable the Committee to meet its mandate. However, it is stated in section 5 of the Monitoring Instructions that the Committee shall not apply for more extensive access to classified information than is necessary for purposes of monitoring, and shall as far as possible observe consideration for the protection of sources and of information received from abroad. Pursuant to section 6 of the Instructions, it is nevertheless the Committee that decides what information it shall apply for access to, although the responsible personnel at the duty station concerned may require that a reasoned protest against such decisions be recorded in the minutes.

In 1998, the *Storting* considered a number of issues concerning the Committee's inspection of the Norwegian Intelligence Service and, in this connection, the application of the aforementioned sections 5 and 6 of the Committee's instructions. The background was a dispute between the Committee and the Service concerning access to certain information. The *Storting* then provided guidelines for the Committee's exercise of the right of inspection in the Norwegian Intelligence Service, and stated that, in the case of a dispute concerning access to information in this Service, the matter shall be submitted to the Minister of Defence and, if necessary, be brought before the *Storting*. A special arrangement has thus been established on the basis of the special confidentiality considerations that apply in this service. No subsequent disputes have arisen concerning access to information, and it has therefore not yet been necessary to implement the terms of the special arrangement.

*The Committee's Duty of Secrecy*

Much of the information received by the Committee in its monitoring work and in investigations of complaints is classified, that is, subject to secrecy in the interests of national security. Classified information may not be disclosed by the Committee. This sets clear limits for the type of orientation or information the Committee can provide to complainants concerning its investigations and their results. In connection with complaints against the surveillance activities of the Norwegian Police Security Service, the Committee may in general only rule on whether or not the complaint contained valid grounds for criticism. Nor may the Committee, pursuant to the Act, inform a complainant as to whether he or she has been registered or subjected to surveillance, since such an arrangement would enable anyone to ascertain whether he or she was the subject of the service's attention. The Committee may however request the consent of the service

17. Section 4 of the Act relating to the Monitoring of Intelligence, Surveillance and Security Services.

concerned or the Ministry to provide a more detailed explanation in a specific matter if this is found to be particularly necessary. This right has been exercised in several cases, in relation to both the Police Security Service and the Norwegian National Security Authority, and has enabled the Committee to provide complainants with a more informative explanation than would otherwise have been possible. So far there have been no leaks by the Committee.

*The Committee's Reporting*

Pursuant to section 8, subsection 2, of the Act relating to the Monitoring of Intelligence, Surveillance and Security Services, the Committee shall, by 1 April each year, submit a report to the *Storting* concerning its activities during the previous year. If the Committee discovers matters that it considers the *Storting* should be informed of immediately, it can submit a special report on the matter. The reports to the *Storting* are public. This clearly limits the kind of matters that can be referred to in the reports, and how such matters can be broached. This constitutes a constant challenge for the Committee. It is important to provide the *Storting* and the general public with a certain insight into what the activities of the services consist of. Yet at the same time, it is necessary to avoid disclosing classified information. Before submitting the report to the *Storting*, the Committee confers with the services to ascertain whether certain information contained in the report is suitable for release. In this way, the Committee is able to ensure that classified information is not disclosed.

If the Committee believes that a case of concern to the *Storting* contains classified information, it can bring this to the attention of the *Storting*.[18] However, such a communication must also be free of classified information. The further treatment of such a communication must be a matter for the *Storting*. The Committee thus has no right to communicate classified information to the *Storting* on its own initiative.

It has been decided that, if the *Storting* wishes to obtain classified information on a matter on the basis of a communication from the Committee pursuant to section 13, subsection 2, of the Instructions (or on some other basis) it must request that the government provide the information concerned. This memorandum entails that it will never be appropriate for the Committee to submit classified information to the *Storting*, even classified letters sent by the Committee to the services in connection with individual cases are precluded.

In individual cases, questions have arisen concerning the Committee's reporting to the *Storting*. In 1998, the Ministry of Defence forwarded certain classified documents to the *Storting* concerning a matter that the Committee had dealt with, but omitted to enclose the views expressed by the Committee. This situation was found to be unsatisfactory by the Committee. The specific case was dealt with but the fundamental issue remains unresolved.

The current regulations and the procedures outlined constitute an arrangement that is simple for the Committee to exercise. The arrangement does

18. This is stated explicitly in section 13, subsection 2 of the Monitoring Instructions.

not in itself represent a problem, and it should be noted that a request from the *Storting* to the government to provide classified information concerning a matter will result in the full provision of that information. In principle, it can nevertheless be argued that it would be advantageous for the Committee in special cases to be able to provide the *Storting* with classified information. The Committee may find itself in a situation where there is nowhere for it to go with information that it regards as important to bring to the attention of the *Storting*. However, the current rule is clear, and is now firmly established, given that the *Storting* considered the issue in 2001 and decided that the rule should not be amended.

## Oversight in Practice

The Committee exercises oversight in two ways: by means of inspection activities and by dealing with complaints and cases that it raises on its own initiative. It is the inspection activities that constitute the most important part of the oversight. Compared with the oversight arrangements of other countries, it seems that it is the emphasis on inspection activities that particularly characterises the Norwegian oversight arrangement. However, dealing with complaints is also an important oversight function, since it opens a channel into the secret services for ordinary citizens who believe themselves to be unjustly treated by the services.

### *Inspections*

Section 3, first paragraph, of the Act relating to the Oversight of Intelligence, Surveillance and Security Services states that the Committee shall regularly monitor the services, and section 4 of the Act lays down the Committee's right of inspection and right of access to the services' archives, registers, premises and installations. Section 11 of the Oversight Instructions provides detailed regulations for the exercise of inspection activities. The provision specifies the minimum number of inspections that must be held annually in each of the services, both centrally and locally, and the factors that must deserve particular attention.

The Committee inspects the headquarters of the Norwegian Police Security Service six times a year, the Norwegian National Security Authority four times a year and the Norwegian Intelligence Service twice a year. If necessary, more inspections can be conducted. External duty stations of the services are also regularly inspected. Advance notice of inspections is given. Unannounced inspections can also be held, but are not the usual practice of the Committee.

### *The Police Security Service*

The Police Security Service is led by the Central Unit. The Service has units in all of Norway's 26 police districts. The central responsibilities of the Service involve prevention and investigation of unlawful intelligence activities, terrorism and the spreading of weapons of mass destruction. The Committee's inspection of the Norwegian Police Security Service is particularly focused on the criteria and

practice surrounding the maintenance of the Service's registers for preventive purposes, for release of personal data to others and in general for updating and clearance of archives and registers. Oversight also includes the Service's investigative activities, including the use of various methods such as wiretapping. The Service and its oversight activities are primarily directed towards persons.

Issues the Committee has shown particular interest in including clarifying requirements regarding the information that is registered, so that it is possible for the Committee to see from what is registered what the legal (or professional) grounds are for the registration. Furthermore the Committee has focused on ensuring that the Service itself maintains a clear overview at all times of its own working registers – that is registers or databases containing personal information about individuals, both in local units and in each division of the Central Unit. The information in all of the Service's working registers shall be evaluated after it has been registered for five years, and shall as a general rule be deleted if nothing new has been added about the person concerned since the first registration.

Special mention should be made of the release of personal data to other bodies. In connection with vetting for security clearance, the registers of the Police Security Service are also checked. Since refusal or withdrawal of security clearance can result in the loss of employment as well as career and educational opportunities, it is required that only information that has been quality-controlled and that is regarded as relevant for security is released to the clearance authority. The Committee is continuously concerned with this, and has dealt with several cases where it has asked questions about the quality and relevance of released information. After 9/11, the Committee has also placed greater emphasis on monitoring the release by the Police Security Service of personal data to other countries' services.

In order for the Committee to exercise genuine control, it is necessary that the services put down in writing their decisions and activities, and that they have proper procedures for this. For example, the Committee dealt with a case in 2001 concerning the investigation of a journalist for suspicion of espionage for the former German Democratic Republic (GDR). The Committee criticised several aspects of the Police Security Service's handling of the case, which was finally dropped after an extensive and time-consuming investigation. Criticism was voiced over the failure of routines regarding seized materials as well as deficiencies in internal information routines and the supply of information to the person charged and his defence lawyer.

As previously explained, the superior prosecuting authority is exempt from oversight by the Committee and in this case questions arose as to which activities were the responsibility of the Police Security Service and which were to be decided by the superior prosecuting authority. The reason for this discord was that there proved to have been extensive oral communication between the Police Security Service and the superior prosecuting authority during the course of the investigation. In response to the Committee's questions about the source of various decisions, such informal communication was often referred to. In its concluding statement, the Committee commented on these circumstances as follows:

> The Committee is responsible for monitoring the Police Security Service's investigative activities as well as its preventive activities. In the case under consideration it has been difficult to maintain a clear idea of which decisions in the investigation have been made by the Police Security Service and which by the superior prosecuting authority. This is due to the fact that the communication between the parts of the prosecuting authorities has mainly been conducted orally, as is confirmed by the Police Security Service, for the most part without any subsequent notes being taken or any formalisation of the case by the Police Security Service as the Committee understands. In the general briefings on the case that have been given while investigations were in progress, the Police Security Service has thus often responded to the Committee's questions by informing that the public prosecutor has been informed, has given his approval, has been consulted and the like.
>
> Owing to the demarcation between the Committee's jurisdiction and that of the superior prosecuting authority, it is problematic to relate to such references of oral communication between parts of the prosecuting authority. As a basis for deciding what is included in the monitoring responsibility, it is, in the view of the Committee, necessary to specify certain formal requirements. The consequence may otherwise be that the Committee's monitoring of the Police Security Service's investigative activities is obstructed owing to oral and non-documental contact between parts of the prosecuting authority. As long as the formal leadership of the investigation is the responsibility of the Police Security Service, the Committee assumes that only those decisions or instructions by the superior prosecuting authority that are put down in writing on the case file have been made by that authority, and fall outside the area of supervision. In the view of the Committee, this must apply regardless of whether it is otherwise normal that considerable informal communication takes place between parts of the prosecuting authority during criminal proceedings (Norwegian Parliamentary Oversight Committee, 2001, p. 10).

The Committee's view was supported by the Director General of Public Prosecutions, who, on the basis of the Committee's statement, enforced requirements regarding formality and written decisions/directions in respect of the public prosecutors and the Police Security Service.

*The Norwegian National Security Authority (NoNSA)*

The Norwegian National Security Authority (NoNSA) is currently organised as a civilian directorate under the Ministry of Defence. The Directorate's responsibilities are of a preventive nature and it does not conduct investigations. The Committee's main responsibility in relation to this service consists of monitoring procedures and decisions in matters concerning security clearance. The Committee's area of supervision includes all of the clearance authorities, both military and civilian. This is a relatively large number of bodies, since clearance authority is assigned to approximately 15 different defence authorities or divisions, and to approximately 40 different agencies. The Norwegian National Security Authority is the appeal body for all of these clearance authorities. In connection with its inspections of the Norwegian National Security Authority, the Committee is regularly shown all appeal decisions where the appeal did not succeed. In

addition, the Committee makes regular random controls of decisions concerning refusal or withdrawal of clearances where appeals were not made.

Another important responsibility of the Committee is to ensure that the service's preventive monitoring of communications occurs within the boundaries of the framework laid down in the Security Act and regulations issued pursuant to the Act. NoNSA's surveillance of communications involves the monitoring of an institution's telephones, and/or data communications (for instance, a ministry or defence division), in order to control whether classified information is communicated contrary to security legislation. This includes a prohibition against the monitoring of private communications and a requirement that all material shall be deleted within given time limits. Communications monitoring may only be implemented on the prior consent of the institution's senior staff, which is required to inform all employees.

Oversight of this service by the Committee particularly includes monitoring of the possibility for clearance applicants to obtain access to the grounds for negative decisions in security clearance cases. Without such access it is difficult for parties to receive a fair hearing. This is an issue to which the Committee has devoted considerable effort, both in general and in relation to several individual cases. Such a case concerned a civilian employee at Headquarters Defence Command Norway, whose security clearance was withdrawn owing to a failure of document security in the office of the person concerned. With regard to the part of the case that concerned right of access and right to a fair hearing, the Committee stated in its report to the *Storting* for 2000:

> The Committee concluded its handling of the case with a letter to the Ministry of Defence. The Committee complained that the party had not been allowed access to the background documents for the decision, which had resulted in his being given in reality limited potential to safeguard his interests while the case was being dealt with. The Committee pointed out that the party by all appearances would lose the post he had held for many years if he were deprived of the security clearance, and that strict demands should therefore be made of the handling of the case. Without access to the central case documents, the party had only a very limited potential for safeguarding his interests in the case. It was, for example, not possible for him to oppose the evidence for the individual violations (Norwegian Parliamentary Oversight Committee, 2000).

During the consideration of the annual report by the *Storting*, the Minister of Defence admitted that there had been a failure of routines regarding access to information in this case, and signalled an amendment of the practice for granting access to information in security clearance cases. Following this case, access to information is granted to a greater extent than it was previously.

*The Norwegian Intelligence Service*

The Director General of the Norwegian Intelligence Service is the Chief of Staff of Headquarters Defence Command Norway/Intelligence Division (FO/E). The activities of the Service were regulated by law in 1998, which resulted in increased

visibility and, with that, a certain demystification of the activities of this Service, which have traditionally been shrouded in secrecy.

The Service's legal obligation is to obtain, process and analyse information of importance for Norwegian security interests viewed in relation to foreign states, organisations or private individuals. This means that the activities of the Service are directed against external threats, that is threats outside Norway's borders. The Service operates duty stations for collection and analysis of electronic communications, and has units at the highest military commands. It cooperates with corresponding services in other countries. A main task in the Committee's oversight of the Norwegian Intelligence Service involves ensuring compliance with the prohibition against the surveillance of Norwegian physical or legal persons on Norwegian territory, laid down in the Act relating to the Norwegian Intelligence Service, and that the Service remains under national control. This oversight is characterised by the high level of technology within electronic intelligence. The Committee therefore makes use of expert assistance in monitoring this service.

The development of computer technology and telecommunications is a major challenge for oversight activities in general, but in particular to the oversight of the Intelligence Service. A keyword is convergence, that is the merging of communication channels for different types of communication (telephony, e-mail, radio, and so forth) as a result of digitisation. Oversight, ensuring that the Service keeps within its sphere of operations and its margin of surplus information, is marked by this development.

## Complaints and Matters Raised on the Initiative of the Committee

Anyone who believes that the EOS services may have committed injustices against him or her may complain to the Committee for the Oversight of Intelligence, Surveillance and Security Services. All complaints that fall under the area of supervision and that show a certain basis in fact are investigated. A complaint should be made in writing and sent to the Committee. If this is difficult, help in formulating a complaint may be provided by prior arrangement. It is important that grounds are given for the complaint and that the complaint is made as explicit as possible.

No explicit time limit applies for complaints to the Committee. However, the Committee is cautious of investigating complaints concerning matters of considerable age unless they can be assumed to have current importance for the complainant and it has been difficult to submit the complaint earlier. Complaints are investigated in the service against which they are directed. This is partly carried out in writing, partly orally in the form of inspections and partly by checking archives and registers. Complaints to the Committee are dealt with in confidence but, when a complaint is investigated, the service concerned is informed. If the investigation reveals grounds for criticism, this is indicated in a written statement to the service concerned. The Committee has no authority to instruct the services to take specific action concerning a matter, but may express its opinion, and may make recommendations to the services, for example, to reconsider a matter.

Even if no complaint has been submitted, the Committee shall on its own initiative investigate matters or circumstances that it finds reason to examine more closely in view of its supervisory capacity. It is stressed as being particularly important that the Committee investigates matters or circumstances that have been the subject of public criticism. A not inconsiderable number of the matters investigated by the Committee are raised on the initiative of the Committee.

The handling of complaint cases can best be illustrated by the examples of two cases where the Committee found reason to level a certain criticism against the Police Security Service, and where the Committee received consent to provide detailed grounds.

One of the cases concerned the question of whether a registration that had been made of the complainant could be said to be professionally relevant, which is the basic criterion for registration. Regarding this question, the Committee stated as follows in its concluding letter to the Police Security Service:

> The decisive factor indicating registration is whether, following an expert assessment, the information is regarded as relevant for the activities. This provides a broad and discretionary right to register information. However (as also stated by the Police Security Service) a specific assessment must be made of the relevance of the individual case before information is registered. From the information that was given concerning the case, the Committee is not able to see that the registration on 16 August 1997 satisfies the requirements referred to here. When the Service itself is unable to see from a registration what the professional reason was for making it, it is probable that the requirements as regards expert assessment and clarity concerning what is registered were not satisfied. It can hardly be maintained that such registrations comply with the regulations (Norwegian Parliamentary Oversight Committee, 2002, p. 9).

On the basis of the Committee's statement, the Service decided to delete the registration concerned.

The other case concerned the question of whether it was in compliance with the regulations to obtain a list of participants at a congress for journalists. The attempt to obtain this list had been reported in the press and the Norwegian Union of Journalists complained to the Committee. In its concluding letter to the Police Security Service, the Committee stated:

> Section 4, second paragraph, of the Surveillance Instructions of 19 August 1994 states: 'Membership of a political or other lawful organisation does not constitute a basis for retrieval and registration of information' (Norwegian Parliamentary Oversight Committee, 2002, p. 9).

The provision has as its basis and point of departure that all lawful activities shall be protected from monitoring, registration and surveillance. The Lund Commission formulates this in relation to the somewhat narrower provision in the instructions of 1977 (Lund Report, p. 299), that political affiliation, *inter alia*, in itself does not constitute relevant grounds for surveillance, and that information of this character may only be registered if, in an individual case, there are found to be other

significant grounds for surveillance. In other words, it would have to constitute additional information concerning a person who was the subject of the service's attention for another reason. The Committee adopts this interpretation, which entails that the motive for retrieval is not decisive for the question of whether section 4, second paragraph of the Surveillance Instructions of 19 August 1994, has been violated, but of whether the specific information that is retrieved is found to be relevant from a surveillance or official point of view.

The Police Security Service stated that it had asked for the list of participants in the course of its duty, pursuant to the instructions, to carry out surveillance of foreign visitors. This might, at the most, explain a request for information about the foreign participants at the annual congress. By requesting a list of all participants, the Police Security Service, in the view of the committee, exceeded the constraints provided by section 4. Even if the motive for requesting the list was surveillance of foreigners, it could hardly be regarded as officially relevant to obtain information about Norwegian participants. The Service must be judged on the basis of its acts, not the motives or aims that underlie them.

It may be asked whether retrieval of information about all foreign participants to the congress could be regarded as relevant to work on immigration control, even if this provided the Service with information concerning their affiliation to an international cooperation or interest organisation for journalists, that is information that in the circumstances falls within the scope of section 4, second paragraph. The Committee's area of supervision is in principle restricted to persons resident in Norway, and the Committee does not have an intimate knowledge of the methods normally employed by the Police Security Service for surveillance of foreign visitors or of the Service's cooperation with the immigration authorities. The Committee has not found reason for further examination of these matters in relation to this case since the Service has stated that, neither from the organiser nor in any other way, was information obtained about the congress participants.

In its letter to the Committee, the Police Security Service also expressed itself in a way that may be perceived as indicating that the Service holds the view that anti-terrorism contingencies following 9/11 call for a restrictive interpretation of section 4, second paragraph, of the Surveillance Instructions. In that event, this is a point of view that the Committee finds difficult to subscribe to owing to the nature and central importance of this provision. It is precisely at times when barriers of this kind are subjected to pressure that they are important. If the Service regards this provision as an obstacle to efficient anti-terrorism operations, it should request that it be amended.

## Conclusion

The Committee may be said to have contributed to increased awareness of rule of law considerations in the services. This may particularly apply to the Norwegian National Security Authority and the Norwegian Intelligence Service, whose activities were not previously regulated by law. It can certainly also be established

that it is the preventive effect of the Committee's inspection activities that is of greatest importance. The certainty of regular inspections increases the alertness of the services to propriety.

Externally, the Committee has primarily gained the approval, both of the services in its handling of individual cases, and of the *Storting* in connection with consideration of the Committee's reports. The previously mentioned case relating to access to information concerning the Norwegian Intelligence Service resulted in a dispute concerning the Committee's handling of the matter, which may have weakened the Committee's position somewhat. However, in 2001, the *Storting* assessed the whole arrangement concerning the Committee for the Oversight of Intelligence, Surveillance and Security Services. A unanimous *Storting* then expressed satisfaction with the work of the Committee, and no amendments were made in the oversight regulations.

# PART IV

# Parliamentarians

*This page intentionally left blank*

Chapter 10

# Parliamentary and External Oversight of Intelligence Services

*Hans Born*

## Introduction

There could scarcely be a more appropriate time to address the issue of the oversight of security and intelligence services. In the wake of the events of 9/11, the Iraq war, the bombings in Madrid on 11 March 2004 and in London on 7 July 2005, many of those responsible for overseeing intelligence in both the legislative and the executive branches of government are currently involved in investigating the intelligence services and the way political leaders use or misuse the intelligence they receive. The United States (US) 9/11 Commission[1] and the United Kingdom (UK) Butler Commission,[2] to mention just two inquiries, have dealt with formidable questions indeed: are intelligence officials working effectively and within the rule of law? Do political leaders politicise intelligence? Do intelligence services need additional legal powers and resources in order to deal with terrorist threats? These and other questions illustrate that the process of intelligence oversight has two important goals in democratic societies: keeping the services in line with their legally defined mandate, respect for human rights and ensuring their effectiveness.

A basic question concerning the democratic control of intelligence services is how to maintain public control of services which must operate – to a certain extent – in secrecy. For a better understanding of this elementary question, this chapter compares how parliaments are involved in the oversight of intelligence services in eight selected democratic states, that is: Argentina, Canada, Norway, Poland, South Africa, South Korea, the UK and the US.[3] These states are selected because they have all established a form of external and parliamentary oversight, and because their intelligence services function on the basis of a statutory law, enacted by parliament (as opposed to services which operate on the basis of

1. National Commission on Terrorist Attacks Upon the United States, 2004.
2. Report of a Committee of Privy Counselors, 2004.
3. This chapter draws on an earlier publications, Hans Born, 2004; Born and Leigh, 2005; Born, Johnson and Leigh, 2005.

executive decrees).[4] Furthermore, the states represent a diversity of various political presidential and parliamentary systems, they are located in various continents (America, Europe Africa and Asia) and they represent both established and post-authoritarian democracies.

The decision to focus on parliaments is based on the fact that parliaments symbolise that 'normal' democratic decision making procedures apply not only to government activities such as education and health, but also to the special secretive field of intelligence services. It equally symbolises that control of the services is not only a matter of control of a small group of experts, who do their work out of the eye of the public, but that the control is widened to include representatives of the people. A better understanding of parliamentary oversight of intelligence services leads to insights into how democracies around the world overcome the paradox of the need for accountability and transparency *vs* the need for secrecy.

After having elaborated on the relevance of parliamentary oversight, the concepts of intelligence and democratic control, this chapter turns to a comparison between the powers and procedures of parliamentary and external oversight in the selected states.

## The Need for Parliamentary Oversight of the Intelligence Services

Why is it important to include legislators in the general process of ensuring intelligence accountability? Four reasons stand out. *Firstly*, the danger exists that intelligence may be abused by intelligence officers. In reporting on the conduct of the intelligence services, parliamentarians are providing a security check to avoid this. *Secondly*, an equally likely and often more dangerous scenario is the abuse of intelligence by the executive branch. As mentioned before, the so-called 'politicisation of intelligence' for partisan purposes has become a central theme following the war in Iraq in 2003, yet the danger is not new and it requires institutional safeguards. In the US and the United Kingdom, many of those responsible for overseeing intelligence in both national legislative bodies are currently involved in investigating the functioning of the services, as well as the conduct of political leaders responsible for tasking and directing the services. Parliamentarians are needed to guarantee a viable system of checks and balances that prevents one branch of the state from dominating the others. *Thirdly*, legislators – the elected representatives of the people – authorise the budget for the intelligence services. As this concerns taxpayers' money, it is, of course, necessary that parliamentarians be included in the budgeting process. *Fourthly*, parliament, on behalf of the people it represents, has to check whether human rights are respected both in theory and in policy, as well as in practice and in the intelligence services' operations.

4. Canada's oversight body – the Security Intelligence Review Committee (SIRC) is strictly speaking not a parliamentary oversight body, but is included as it represents an interesting option for robust, external and independent oversight of intelligence services.

**Intelligence**

Often regarded as the second oldest profession, intelligence has become a crucial factor in a state's security and foreign policy (Knightley, 1988). Security and intelligence services are a key component of any state, as they fulfil four essential functions: (1) to warn of surprise strategic threats; (2) to provide long-term expertise; (3) to support the decision-making process of policymakers; (4) to maintain secrecy of information, sources and methods (Lowenthal, 2003, pp. 2–5). Especially in the post-Cold War era, which is characterised by asymmetrical threats, surprise attacks by terrorist organisations, and civil wars with dangerous and unexpected spill over effects, there is a greater need for, as former US Defense Secretary Donald Rumsfeld put it, 'exquisite' intelligence.[5] Getting better intelligence, therefore, is essential and should be one of the tasks of the overseers of the intelligence services in the legislative and executive branches. This necessary task is rendered more difficult by the inherent challenges of monitoring terrorist cells and networks of secret terrorist organisations, which are highly mobile and fluid.

Without effective intelligence, the pre-emption and prevention of expected attacks from rogue states and terrorist cells are impossible. Legislators have to ensure that recommendations for improving security and intelligence services are implemented, notably: more intelligence gathering from human intelligence sources (HUMINT) instead of relying on communication intercepts and satellite images; promoting creativity and fostering criticism instead of rewarding risk avoidance and conformity; and harmonising policymaking and intelligence (Gormley, 2004, pp. 7–28).

In daily life, the word *intelligence* is used in many different ways. In a democratic society, however, it is important to limit the mandate of the intelligence services to cover only dangers and potential dangers to national security. If security and intelligence services are given functions in other aspects of daily life – for example, public transportation, internet communication, or education – a real danger exists that too many aspects of society will become 'securitised', which turns the state into a so-called *security state*. National security should be distinguished from regime security, which relates to the protection of a particular political regime against its own people. National security, on the contrary, not only relates to the protection of the state but also to the protection of the individual citizens of that state.[6]

---

5. *Nuclear Posture Review [excerpts]*, 15, available at: http://www.globalsecurity.org/wmd/library/policy/dod/npr.htm. Unfortunately, the last two Iraq wars have shown the limitations of intelligence. In the first Iraq war, American intelligence underestimated Saddam Hussein's weapons of mass destruction (WMD) programs, whereas in the second Iraq war the CIA overestimated Hussein's WMD capabilities.
6. Council of Europe – Venice Commission, 1998.

What is intelligence? In government, intelligence usually has a restricted meaning – it has particular associations with international relations, defence, national security, and secrecy: and, of course, with specialised institutions labelled 'intelligence' (Herman, 1996). Intelligence can be described as a 'kind of knowledge' and 'activity pursued by the intelligence organisation' thus an intelligence organisation can be described as 'the type of organisation which produces the knowledge' (Kent, 1965, p. xxiii). Because the functioning of intelligence services is based, ideally, on a legally defined mandate and is subject to civilian political leaders' control, it is important that the worlds of intelligence and policy remain close, but not too close, as this might lead to the politicisation of intelligence.

**The Risk of Politicisation of Intelligence**

Intelligence is 'information that meets the stated or understood needs of policymakers and has been collected, refined, and narrowed to meet those needs' (Lowenthal, 2003, pp. 1–9). Intelligence is useless if it is created too late or is not related to a government's policy agenda. Though it is important that intelligence production be tailored very closely to the needs of policymakers, it is important that it not be politicised, meaning that intelligence reporting should not be shaped to support decisions that have already been made by the administration in power, or, more crucially, that intelligence should never be used against political opponents. Politicisation of intelligence is likely to occur if:

- intelligence is serving politics instead of policymaking (for example, if threat warnings are used to support a governmental campaign during election periods);
- the administration is able to alter intelligence reports;
- intelligence units are set up for specific political purposes;
- intelligence officers and their Directors are political appointees or publicly affiliated to political parties;
- and, a system of checks and balances between the various governmental branches is lacking or poorly developed, leading to a situation in which one of the branches might dominate the intelligence services.

Intelligence officers are supposed to report to policymakers in an objective, balanced, timely, and professional manner. In order that intelligence services be capable of 'speaking truth to power', the services should be insulated but not isolated from politics.

**Democratic Oversight of Intelligence Services**

Needless to say, national oversight practices vary greatly according to how much power is granted to intelligence services and how they are held accountable for their actions. Accountability for governmental actions is a key requirement in a democracy. Government officials, including intelligence employees, are required to answer to the elected representatives on the disposal of their powers and duties and must act upon criticisms or requests made of them. Government, including the intelligence services, must accept responsibility for failure, incompetence, or deceit.

But how is intelligence accountability best achieved in practice in a liberal democracy, and which actors should be involved in the process? Although secrecy is a necessary condition of the intelligence services' work, intelligence in a liberal democratic state needs to work within the context of the rule of law, checks and balances, and clear lines of responsibility. Democratic accountability, therefore, identifies the propriety and determines the efficacy of the services under these parameters. Based on earlier research (Born and Leigh, 2005), a five-fold classification of state and non-state overseers most appropriately captures the different layers of intelligence accountability:

- Executive control;
- Parliamentary oversight;
- Judicial review;
- Internal control;
- Independent scrutiny.

According to this classification, the executive controls the intelligence services by giving them direction – including tasking, prioritising, and making resources available. The legislative or parliamentary branch is also an indispensable actor, as it focuses on the oversight of the intelligence services primarily by enacting laws, examining the decisions and actions of the services, and authorising the budget for the intelligence services. The judiciary is tasked with monitoring the use of special powers (and, if necessary, prosecuting possible misconduct by intelligence officers). The intelligence services themselves are assigned the task of providing internal safeguards within the chains of command to prevent the abuse of intelligence by staff members. Last but not least, civil society, think tanks, the media, and individual citizens restrain the functioning of the services by offering an alternative view of the appropriate tasks for the intelligence services, disclosing scandals, and by issuing complaints in cases of wrongdoing. There is, of course, no fail-safe method of ensuring intelligence accountability; however, the interdependence of all five stages in the process offers the best guarantee of a successful result.

Control and oversight are two different concepts. Arguably, control refers to the act of being in charge of the day-to-day management of the intelligence services. The responsibility for control of the intelligence services is held by the

executive, not by the legislature. Oversight as exercised by the legislative branch involves a lesser degree of day-to-day management of the intelligence services, but requires an equal amount of scrutiny. There is a thin dividing line between government and parliament. Parliament exercises oversight, whereas government is tasked with control. These tasks are *not* the same: the executive ultimately has to decide how far their oversight should reach.

It is important to stress that, in a democracy no area of government can be barred from the oversight of parliamentarians. Today, it is not only normal but critical that parliamentarians exercise oversight over their national intelligence services.

## Comparing Practices of Executive and Legislative Oversight

As already indicated, national practices vary substantially with regard to the extent of the mandate, budget-control powers, number of members, appointment and clearance procedures of the parliamentary oversight body. A previous study carried out by DCAF, the Norwegian Parliamentary Intelligence Oversight Committee, and the Human Rights Centre of the University of Durham, compared the laws and practices of parliamentary oversight bodies in eight different countries. The main findings are shown in Table 11.1 and cover, as mentioned earlier, Argentina, Canada, Norway, Poland, South Africa, South Korea, the United Kingdom, and the United States.

## Parliamentary Oversight as a Recent Development

Table 10.1 shows that parliamentary oversight committees have existed only in the last two decades, revealing that the 'parliamentarisation' of the oversight of intelligence services started only recently both in new and old democracies. Indeed before the mid 1970s, parliamentary and external oversight of intelligence services hardly existed.[7] Four reasons can be found why states started to put in place mechanisms of parliamentary oversight of intelligence services. Firstly, in many countries the process of parliamentary oversight began as a response to scandals which were exposed by the media and independent external and/or parliamentary investigations. For example, in the US, oversight legislation was enacted by Congress after it became clear in January 1975 that the FBI had been (among other things) spying illegally on anti-Vietnam war protesters in the mid-1970s.[8] Other examples are Canada, Australia, and Norway. A common line connecting these individual cases of scandals followed up by inquiries and legislation, is an

7. Exceptions confirm the rule and the exceptions are the Netherlands and Germany who started earlier with parliamentary oversight of intelligence services in 1953 and 1956 respectively.
8. See: United States Senate, *Final Report*, 1976; Loch Johnson 2005, in Born, Johnson and Leigh 2005.

increasing belief among legislators and the public that the special powers of the intelligence services cannot only be used to protect national security, but can also threaten democracy. These threats may range from intrusive surveillance which erodes civil liberties, attempts to manipulate the political process, to infiltration of pressure groups and unions as well as, in extreme cases, staging coups and conducting extrajudicial killings abroad. Apart from these scandals, the other three reasons can be found in (sometimes overlapping) constitutional reform (for example in South Africa), transition from authoritarian to democratic rule (for example, Poland, South Korea and Argentina) as well as legal challenges (for instance the UK, Netherlands and Romania).[9] In 2006, parliamentary oversight of intelligence services has become an international norm and standard practice for democracies. Most democracies have put their services under statutory law and made them subject to parliamentary and external oversight, with some notable exceptions such as France and Turkey.

Five major features of parliamentary intelligence oversight committees are discussed in this report: the mandate, type of committee, budget-control powers, investigative powers and access to classified information. To a large extent, these five features determine the oversight body's effectiveness, because they guarantee comprehensive oversight, they ensure that parliament has ownership over the oversight committee as well as major instruments of oversight, and – last but not least – that parliament has access to classified information.

## Broad *vs* Narrow Mandates of the Oversight Body

The mandates of the parliamentary oversight bodies vary widely. In some countries, the oversight body has a broad mandate, which includes policy and operations as well as the legality and efficiency of the services (examples include the US, South Africa, Canada, and Argentina). In other countries, the intelligence services are only partially reviewed by the oversight bodies. For example:

- The Norwegian committee focuses on human rights protection and whether the services respect the rule of law;
- The UK committee deals with policy and administration mostly, but does not cover operations nor the legality of the services' functioning;
- The Polish intelligence oversight committee does not address effectiveness of the services.

These oversight committees have a narrow mandate, with the risk that oversight is imperfect or fragmented across different institutions (for example courts) and oversight committees.

9. Leigh 2005, pp. 3–5, in Born, Johnson and Leigh, 2005.

**Table 10.1 Comparison of the External and Parliamentary Oversight Bodies in Eight Selected Countries**

| Country | First Oversight Legislation | (1) Mandate of Oversight Body | (2) Type of Oversight Body: # Membership, Clearance, Appointment | (3) Budget-Control Powers of Oversight Body | (4) Investigative Capacity | (5) Access to Classified Information |
|---|---|---|---|---|---|---|
| **(A) Argentina** | 1992 | Reviews legality and effectiveness of the services, including citizens' complaints. | Parliamentary oversight body of 14 MPs, appointed by parliament. No security vetting. | Both scrutiny and authorisation powers. | Committee can initiate investigation based on a complaint or on conclusions of its own work. | Full access. |
| **(B) Canada** | 1984 | SIRC checks legality and efficacy of the agency. | External independent expert oversight body of max. 5 experts, appointed by prime minister. Members are under oath. | SIRC has no authorisation powers. Can comment on CSIS's budget | Committee decides upon its own work plan | Full access. |
| **(C) Norway** | 1995 | Focuses primarily on legality, including human rights protection. | External expert parliamentary oversight body of max. 7 (non-MPs), appointed by parliament. | No budget oversight function. | Can investigate what it chooses within its mandate. | Full access. |
| **(D) Poland** | 1995 | Oversees legality, policy, administration and international cooperation. Effectiveness is not checked. | Parliamentary oversight body of max. 9 MPs, appointed by parliament. Members are vetted. | Commission scrutinises the services' draft budget and its implementation. | Commission lacks investigative powers. Criticised for lacking own initiatives. | Dependent on the discretion of the services. |
| **(E) South Africa** | 1994 | Includes legislation, activities, administration, financial management and expenditure. | Parliamentary oversight body of 15 MPs, appointed by president. Members are vetted. | Committee does not oversee the intelligence services' budgets, but its purview includes financial management of the services. | Committee has broad and intrusive powers. | Full access except on sources. |
| **(F) South Korea** | 1994 | Examines and comments on legislation and effectiveness. Holds hearings on nominations for senior positions in the NIS. | Parliamentary oversight body of 12, nominated by political parties. | The Committee has no budget powers. | Meagre use of its investigation powers. | Full access under law, but poor service track-record in practice. |
| **(G) United Kingdom** | (1989) 1994 | Finance, administration and policy of MI5, MI6 and GCHQ with a view to efficiency. Does not check legality | Parliamentary oversight body of 9 drawn from both Houses of parliament, appointed by the prime minister | Committee scrutinises the finances together with the Public Accounts Committee but has no authorisation power. | Can investigate what it chooses within its mandate | Full access but some 'sensitive' material can be refused. |
| **(H) United States** | 1974 | Reviews all intelligence agencies. Approves top intelligence appointments. Checks both legality and effectiveness. | Two Congressional oversight committees, of 20 (House) and 17 (Senate) Congressmen, appointed by House and Senate leaders | Both Oversight Committees possess authorisation and appropriation powers. | Yes, e.g. Boland Amendments dealing with covert action (in Nicaragua) | Full access. |

*Source:* Born, Johnson and Leigh, 2005, pp. 230–237

In addition to the distinction between broad and narrow mandates, the mandates of the oversight bodies can also be categorised into proactive *vs* reactive mandates. A proactive mandate is a mandate that allows the oversight body to veto or to alter the policy or functioning of the services before the policy or operation is put into practice. For example, the US Congressional Oversight Committees have the right of prior notification of covert operations.[10] In the US and some other countries, such as Argentina, the parliamentary oversight bodies have far-reaching budget control powers, enabling them to alter policy priorities. Due to prior notification and authorisation requirements, the parliamentary oversight body becomes co-responsible, which might hinder its oversight function due to a lack of critical distance between parliament as a controlling body *vs* parliament as an authorising body. Parliamentary oversight bodies with a reactive mandate (such as those in Norway, Canada, and the UK) do not have this problem. They check the executive's policy and operations after the fact; therefore, parliament cannot be held responsible for a failure of executive policy.

**Committee Type and the Issue of Ownership**

The sample of countries represented in Table 10.1 shows that two types of oversight bodies exist: external expert oversight bodies and parliamentary oversight bodies. The external oversight body exists in Norway and in Canada. These oversight bodies are staffed by experts or by individuals held in high esteem (former ambassadors, ministers, parliamentarians) with expertise in the field of national security and intelligence. In the Norwegian case, the members are appointed by parliament, and the committee reports to parliament. In Canada, its members are appointed by the Prime Minister, after consultation with parliamentary faction leaders, and the committee reports to the responsible Minister, who then reports to parliament. The members of the oversight body of the other countries are parliamentarians, in some instances appointed by and reporting to parliament itself (as in the US and Argentina), and in other cases appointed by and reporting to the Prime Minister (as in the UK).

Which is better – an external expert oversight body or a parliamentary oversight body? One might argue that an external expert body has the advantage of being able to devote more time to and become more specialised in intelligence issues than parliamentarians can. On the other hand, a body whose members are parliamentarians might have more democratic legitimacy, which can facilitate effective oversight.

Perhaps the most important issue is whether the parliament has total ownership of the oversight body – that is, whether parliament alone decides about the body's membership, reporting requirements, and agenda. From this point of view, the oversight systems in the UK and Canada can be regarded as less

10. Except in cases of emergency, in which case the agencies can delay reporting for two days.

favourable, as the Prime Minister can censor the body's reports (as in the UK) and decides about appointments.[11]

### The Power of the Purse

The power of the purse is one of parliament's most powerful tools. In liberal democracies, as a matter of principle, parliament has budgetary-control, because parliamentarians are the representatives of the taxpayers. In some of the selected countries, the oversight body does not have this power. Sometimes this is a matter of division of labour between the parliamentary intelligence oversight body and the parliamentary budget control committee or (parliamentary) independent audit offices (for instance in Norway, the UK, and Canada). In other countries, the parliament clearly lacks this power (for example in South Korea). Budgetary control requires that the parliamentary oversight body has access to all relevant classified budget documents (see below). As far as could be verified in this regard, the oversight committees of these countries do have access to information related to classified programmes and spending. Another important issue, not mentioned in Table 10.1, is the need for having independent audit offices with access to all relevant classified budget documents. Independence from the executive is normally guaranteed by having the Audit Office Director appointed by and reporting directly to the legislative body.

### Investigative Powers

Except for Poland and South Korea, the oversight bodies of the selected countries have included in their mandates the capacity to initiate inquiries. Inquiries need to be bolstered by subpoena powers. If a committee does not have the power to force citizens or civil servants to appear before the committee under oath, it could substantially limit the efficacy of an inquiry, especially where scandalous or sensitive issues are concerned. In the selected countries, the research shows that the oversight bodies of four of the eight countries do not have subpoena powers (these being Argentina, Poland, South Korea, and the UK).

Investigative powers are very important in the case of scandals or of intelligence failures. Particularly, in the wake of 9/11, various countries have carried out public and parliamentary special investigations into the failings or misconduct of intelligence services in the fight against terror and the wars in Iraq and Afghanistan. Prominent examples include the congressionally appointed Kean Commission in the US; the Hutton inquiry in the United Kingdom; the 'Arar' Commission in Canada; the German special parliamentary inquest; and the Dutch

11. In 2003, the Canadian government acknowledged that the current situation is undesirable, as it leads to a 'democratic deficit'. Therefore, the government has called upon parliament to have its own parliamentary oversight committee. See Farson, 2005.

parliament's request to investigate the alleged torture practices of the Netherlands Military Intelligence Service in Iraq.[12] In these special inquiries show that basically two models for inquiries into the functioning of intelligence services are followed: (1) parliament requests independent investigation, carried out by experts, for example, the aforementioned investigations in the Netherlands and the US; (2) parliament requests and conducts the investigation, for example, in Germany. In all cases, these special inquiries are proof that political leaders are no longer convinced that internal investigations are sufficient and instead require public accountability.

**Access to Classified Information**

In order to exercise comprehensive oversight, parliament needs to have access to all relevant documents, including those containing classified information. The oversight bodies of four out of the eight selected countries have unlimited access to classified documents. In the other four countries – Poland, South Africa, South Korea, and the United Kingdom – access is restricted, either because the oversight body is dependent on the cooperation of the executive (Poland and South Korea) or the services are not required to disclose sensitive material on sources and methods (UK and South Africa). In general, if parliament has limited access to classified documents, it is parliament itself who is to blame. The reason is that the classification of documents is based on laws enacted by parliament (so-called 'official secrets acts'), and, therefore, parliament can choose to amend or to reject laws that are overly restrictive.

Having access to classified information means that the members of the oversight body are within 'the ring of secrecy' and clearly facilitates scrutiny of the intelligence services. The flipside, however, is that parliamentarians become silenced as they are not allowed to discuss classified information in public. Especially for parliamentarians this constitutes a major problem as their re-election

12. The Kean Commission, also known as the 9/11 Commission, investigated the circumstances which led to the 9/11 attacks, including levels of preparedness for potential terrorist attacks, see http://www.9-11commission.gov/; The Hutton inquiry investigated the circumstances surrounding the death of Dr. David Kelly in the context of the controversy and debate over whether the Government dossier on weapons of mass destruction allegedly in the possession of Iraq was of sufficient scope and quality to justify the government declaration that Saddam Hussein posed a national security threat to the United Kingdom, see http://www.the-hutton-inquiry.org.uk/index.htm; The mandate of the German Parliament's Committee of Inquiry of 7 April 2006 be found at:
http://www.bundestag.de/ausschuesse/ua/1_ua/auftrag/auftrag_engl.pdf;
The Dutch public inquiry followed press revelations that the Netherlands' Military Intelligence Services used interrogation methods against Iraqi suspects (in Iraq) which amount to torture, see Jan Hoedeman and Theo Koelé, 'Kabinet gelast onderzoek ontsporingen in Irak' [Cabinet requests investigation into derailments in Iraq], *De Volkskrant*, 19 November 2006.

depends on being heard by the media and the public. Alternately, it creates inequality between those parliamentarians who are on the intelligence committee and others who are not on the committee. Those who are not on the committee have to trust their colleagues that they do a good job, but this trust cannot be verified. For these reasons, parliamentarians often make no the use of their right of access to classified information as it might comprise their independence. For example, only a dozen of all 435 members of the US House of Representatives choose to read the classified sections of the Intelligence bill in April 2006, therefore, voting in favour or against the bill without knowing its contents.[13] This problem calls into question how parliamentarians are able to provide oversight of intelligence services if they do not make full use of their powers.

*Attitude of Parliamentarians*

If parliament has access to classified documents, it has the obligation to maintain the secrecy of these documents. Some argue that parliaments do not have the ability to maintain secrecy, because parliament, as an open institution, is ill-suited for discussing sensitive matters. Yet practice has shown that in the selected countries hardly any leaks occur; parliamentary oversight bodies have put special infrastructure and safeguards in place to protect classified information, and committee members are thoroughly vetted. The issue of vetting parliamentarians turns out to be a controversial issue. In some countries, such as the US and the UK, parliamentarians reject vetting, as it would be an indication that they are subject to the executive branch and the security services, which perform the vetting. Other countries (for example, Norway) have decided that the vetting of committee members be carried out by the security services, but that parliament itself is empowered to decide what to do with the vetting results.

## Conclusion

Having a legislature that is powerful enough to counterbalance the executive is necessary in a liberal democracy. An effective system of checks and balances among the legislative, executive, and judicial branches of government avoids the possibility that one branch of the state will dominate the other branches, a situation leading to the potential misuse of security and intelligence services. The main functions of parliamentary oversight of intelligence are to oversee the propriety, efficacy, and legality of the services. The most important tools of parliament in pursuit of these goals are enacting laws, exercising budgetary controls, and inquiring into wrongdoing, failures, and ineffectiveness. Parliamentary oversight is embedded in the broader system of democratic accountability and security sector governance. Democratic accountability mechanisms include procedures and institutions, as well as a political culture that fosters transparency, openness, and an

13. Milligan, 2006.

atmosphere that stimulates parliamentarians and other actors to watch government closely and to observe the security and intelligence services critically.

However, parliamentary oversight does have some inherent dangers. Parliamentarians may draw the security and intelligence services into political controversy or, equally dangerous, an immature approach may lead to sensationalism, conspiracy theories, and false accusations. This could breed cynicism and mistrust among the public about not only the services but also the politicians who are supposed to pursue the common interest. On the other hand, parliamentarians might be unhappy to become members of the intelligence oversight committee, because most of what they work on is classified information, which they are not allowed to discuss with their constituency. Therefore, in terms of re-election, intelligence oversight might prove to be unrewarding for parliamentarians, because they cannot disclose their input or publicise their efforts to support specific classified intelligence policies and operations.

We may conclude that the effectiveness of parliamentary oversight is based not only on the authority (for example, statutory powers) and ability (for example, resources and expertise) of a given oversight body, but also on the courage or willingness of parliaments to hold the government and its services to account.

*This page intentionally left blank*

Chapter 11

# The UK's Intelligence and Security Committee

*Ian Leigh*

## Introduction

Until 1989, the United Kingdom's security and intelligence services were legally and constitutionally invisible. That was the year in which parliament legislated for the Security Service (MI5). Until then, MI5 had rested from its formation in 1909 upon a non-statutory, prerogative basis (see Andrew, 1987, 121 ff.; UK Public Records Office, 1999, 64 ff.).

Up until the Security Service Act 1989, only the sketchiest details were public. Some details were published in 1963 in the report of a judicial inquiry into a notable political scandal (the Profumo affair). This revealed details of the administrative Charter governing the Security Service's work (See *Lord Denning's Report*, 1963), the Maxwell-Fyfe Directive – named after the Home Secretary who issued it in 1952. This brief document emphasised the role of the Service in the 'Defence of the Realm' and its duty to behave non-politically. The Service was, nevertheless, responsible to the Home Secretary and its Director-General had a right of access to the Prime Minister. The Security Service Act 1989 made no change to the constitutional arrangements – the Service was accountable only to Ministers and not to parliament. However the Act did provide an explicit statutory basis for the Service's work and so satisfied the objection that it was unable to conduct surveillance or gather personal information without violating human rights.

The Security Service is the United Kingdom's domestic security agency in effect, although the 1989 Act does not prevent it from acting to protect British interests overseas. It acts under the broad authority of the Home Secretary (the Interior Minister) to protect national security, particularly from threats from espionage, terrorism, sabotage and subversion.[1] The intelligence agency, the Secret Intelligence Service ('SIS' or 'MI6') dates from the same era as its sister agency but was outside the statutory scheme until 1994: indeed until 1992 the government

1. The Security Service Act 1989, s. 1 (as amended) gives the additional functions of safeguarding the country's economic well-being from external threats and of assisting in the prevention and detection of serious crime.

maintained the fiction that it did not even exist. A similar charter was provided for it by the Intelligence Services Act 1994. SIS's primary purpose is to protect national security with reference to the government's defence and foreign policies (Intelligence Services Act 1994, s. 1). It acts under the authority of the Foreign Secretary and may only obtain and provide information or conduct operations against external threats, although it is not prevented from doing so on British soil. The third intelligence agency – Government Communications Headquarters (GCHQ) – was also given a legal mandate by the 1994 legislation. Its remit is signals intelligence and decryption but it also provides protective assistance in these areas and information technology security to government departments and the armed forces (Intelligence Services Act 1994, s. 3).

Unlike the previous legislation, the Intelligence Services Act 1994 acknowledged the concerns over lack of parliamentary oversight by providing for all three agencies a statutory committee of parliamentarians, drawn from both Houses of Parliament.[2] For many, the legal powers of this Committee were a disappointment, certainly by comparison with the systems of oversight in other Westminster democracies that had been introduced in the early 1980s (see also Gill, 1996; Wadham, 1994, p. 916). However, as we shall see, despite its apparent lack of teeth, the Committee has been relatively successful in its first decade (this part of the Act did not come into force until 1995).

## The Arguments For and Against Parliamentary Oversight

Until 1994, successive governments had maintained that necessary secrecy meant that parliament could be told virtually nothing of the work of the security and intelligence agencies. Indeed, remarkably, it was only in 1992 that the Major government had even officially acknowledged the existence of MI6. The 'GCHQ affair' in 1983,[3] in which the Thatcher government removed the right of workers at the signals intelligence agency to belong to a trade union, had drawn attention to that body somewhat earlier.

According to the official argument, the agencies were accountable to the following Ministers respectively, the Home Secretary in the case of the Security Service and the Foreign Secretary in the cases of SIS and GCHQ. The detail of how accountability worked could not (it was said) be revealed without compromising necessary secrets. Parliament and the public therefore lay outside the ring of secrecy and had no alterative but to put their trust in Ministers who were

2. Military intelligence does not have an explicit statutory basis and is not included in the 1994 Act scheme. Although not legally entitled to do so, the Intelligence and Security Committee has exercised a degree of oversight over the Defence Intelligence Staff, for example in its recent inquiry into intelligence leading up to the war in Iraq (below). Lack of authoritative published information prevents further discussion of military intelligence here.
3. The decision was unsuccessfully challenged in the courts: *Council of Civil Service Unions v Minister for the Civil Service* [1985] AC 374.

within it. The government argued that there were insuperable difficulties in the way of true answerability of Ministers to parliament for how they exercised their control.

Accordingly, a convention had grown up of refusing to answer parliamentary questions from MPs on matters concerned with the agencies or touching on national security (Lustgarten and Leigh, 1994, pp. 441–2). Equally, non-disclosure of the money spent by the services had been condoned through the use of the 'Secret Vote' where a global figure was approved annually, without explanation or breakdown of the details (Lustgarten and Leigh, 1994, pp. 447–450). Despite occasional noises of protest from the Home Affairs Select Committee,[4] the work of the agencies had received no attention from parliamentary select committees. The government had indicated that it would refuse to cooperate with any attempt by a select committee to conduct an investigation by not making witnesses available; consequently any investigation would be still-born.

The strength of Westminster-style systems is supposedly that the government is accountable to parliament, since Ministers sit as part of the legislature and so answer directly for the actions of government and of officials. The conventional mechanisms by which accountability is realised are debates, parliamentary questions to Ministers and select committee investigations. In each of these areas, however, accountability for security and intelligence was virtually non-existent due to the restrictions on access to information which successive parliaments had tolerated.

Plainly it would be naïve and inconsistent with maintaining necessary secrecy to expect that operational secrets could be discussed in a public hearing in the parliamentary chamber. Nevertheless, the government's claim of the need for blanket secrecy for the services was unconvincingly over-inclusive. It suggested that nothing could be revealed, even concerning the process of accountability and control of the services' work, or the adequacy of mechanisms to ensure that they stayed within the law. It was plainly unacceptable within a modern democracy for public officials and the use of public finances to be exempt from scrutiny in this way, especially considering the exceptional powers of surveillance and information gathering associated with security and intelligence agencies. When coupled with the traditional deference of the courts to the executive in matters of national security, the effect was to create a vacuum in which the agencies were subject to neither legal nor parliamentary accountability.

Moreover, critics argued that other Westminster-style parliamentary executive systems (notably Canada and Australia) had managed to overcome similar objections to establishing oversight mechanisms. In Canada's case the Canadian Security Intelligence Service Act 1984 created a non-parliamentary committee[5] (the Security Intelligence Review Committee) with a range of oversight and complaints functions, alongside an Inspector-General who reported

4. First Report from the Home Affairs Select Committee, *Accountability of the Security Service* (1992-1993), HC 265.
5. Proposals for a committee of parliamentarians were belatedly made in 2005, Canada, House of Commons, 2005.

to Ministers on the performance of the Canadian Security Intelligence Service (CSIS). In Australia, a statutory parliamentary committee was established with oversight of the Australian Security Intelligence Organisation (ASIO) (the security service) (Australian Security Intelligence Organisation Act 1979; Australian Security Intelligence Organisation Amendment Act 1986), although other agencies (ASIS, the intelligence agency, and DSD, the signals intelligence agency) remained outside this scheme until later reforms (Intelligence Services Act 2001).

The UK government's extravagant arguments for secrecy were not sustainable. Two distinct catalysts for change can be mentioned.

Firstly, there were the revelations of the former Assistant Director of MI5, Peter Wright. The government's protracted but futile worldwide legal attempts to prevent publication of his book *Spycatcher* during 1986–1988[6] highlighted the over-blown nature of the claim that all the work of security and intelligence agencies had to be shrouded in secrecy. In the Australian courts, Wright's lawyers pointed out to devastating effect the many occasions on which MI5 had lifted the veil of secrecy by briefing journalists or condoning or ignoring well-sourced revelations when it suited them to do so. In the ensuing furore the government was unable to demonstrate that it had taken a consistent approach and from that time onwards claims of national security by Ministers have been treated by parliament and the public with considerable scepticism. The European Court of Human Rights subsequently held that the UK courts had breached the right of freedom of expression under the European Convention in suppressing publication by newspapers of Wright's allegations.[7]

Secondly, a further series of legal challenges under the European Convention on Human Rights forced a modernisation of the legal regime governing the agencies. It became apparent that the UK would be found to be in breach of the Convention unless legislation was introduced. Although the ECHR permits restriction of rights such as respect for private life (Article 8 of the Convention) where necessary in a democratic society in the interests of (*inter alia*) national security, this is with the important precondition that the restrictions must be authorised by law. The prerogative basis of MI5's administrative Charter, the Maxwell-Fyfe Directive, was insufficient for this purpose, since it could be changed without reference to parliament and established no formal legal limits or controls. Moreover, the Convention system required there to be some legal mechanisms, even if these did not function in the courts proper, for dealing with complaints about abuses and violations of rights. The 1989 Act established a legal basis for the Security Service and for supervision of the ministerial powers to authorise interference with property (so-called warrants to 'bug and burgle') by a Commissioner, together with a tribunal to which complaints could be brought. This model was followed in the 1994 Act and later modifications. Although the Commissioner and the Tribunal each had very limited powers, a former Director-General of MI5 has commented that is 'difficult to overstate the impact on the agencies of this body of legislation' (Lander, 2004, pp. 481, 484–485).

6. For a detailed account of the litigation: Bailey, Harris and Jones, 2002, Chapter 6.
7. *Observer and Guardian v UK* (1991) 14 EHRR 153.

The government estimated – correctly as it turned out in later challenges – that these token mechanisms would satisfy the Convention system. The mere passing of the 1989 Act, although it came after the events in question, was treated as sufficient reason by the Convention organs to take no further action in two cases brought involving alleged surveillance and recording of personal details by the Security Service.[8] In a later case where the Act's complaint machinery had been used unsuccessfully by an applicant, the Commission of Human Rights found that the statute struck a reasonable compromise between the requirements of defending democracy and the rights of the individual. Accordingly, it held that the complaint was manifestly ill-founded.[9]

Legal change did not at first lead to greater parliamentary oversight. The 1989 Act introduced a Tribunal and a Commissioner but went no further. It was not until 1994 that the Major government acceded to the call for scrutiny by a committee representing a *cross-section* of parliamentary opinion. The Intelligence and Security Committee, established under section 10 of the 1994 Act, comprises nine members drawn from both the House of Commons and the House of Lords, whose task is to examine the expenditure, policy and administration of all three security and intelligence services.

## The Intelligence and Security Committee

### *The Constitutional and Legal Basis of the Committee*

The Intelligence and Security Committee is constitutionally unique. Parliamentary Select Committees are invariably established on a non-statutory basis (under the Standing Orders of Parliament), with membership approved by parliament itself, and reporting to parliament. They do not have legal powers to obtain information in their investigations and depend largely on cooperation with government. The Intelligence and Security Committee is different. It is a statutory committee, which means that it can be less easily abolished or reorganised. Its members are appointed from both Houses of Parliament and by the Prime Minister after consultation with the leader of the opposition. The Committee also reports to the Prime Minister, rather than directly to parliament, although, subject to editing, its reports are subsequently presented to parliament.

In all these respects the Committee is designedly *not* a parliamentary select committee. In view of the way that the Committee has operated and the government has responded these differences may amount to little in practice, but they are intended to underline and reinforce the long-standing argument by governments of all political persuasions that the security and intelligence agencies are accountable to Ministers and not to parliament directly.

---

8. Resolution DH(90) 36 of 13 December 1990. Ironically, the two complainants, Harrriet Harman and Patricia Hewitt are now both ministers in the Blair government.
9. *Esbester vs UK*, App. No. 18601/91, 2 April 1993. See also *G, H, and I vs UK* (1993), 15 EHRR CD 4.

The Committee's statutory brief is 'to examine the expenditure, administration and policy' of the three services (Intelligence Services Act 1994 (hereafter, 'ISA'), s. 10(1)). These terms have been carefully chosen in order to preserve an exclusion zone around security and intelligence *operations*. The legislation impliedly concedes what had previously been denied – that it is possible to separate policy and operational matters in order to allow review by the Committee. However, in a sense the earlier objection is correct: any discussion of policy that is not entirely hypothetical must raise operational issues.

An example will make this clearer. In the wake of 9/11 there have been reports from the US that the Executive Order preventing the CIA from engaging in assassination has been rescinded. The UK government has in the past declared that intelligence officers are not permitted to kill in performance of their duties. Suppose that the Committee wished to explore whether this remains the position. The question would be what limits exist, if any, to the actions in a foreign state that may be authorised by the Foreign Secretary under the 1994 Act (murder is unlawful according to English law under extra-territorial jurisdiction). Is this a matter of policy or operations? The Intelligence Services Act, which deals with ministerial authorisation in section 7, sets no limits. If the Foreign Secretary had informed MI6 and GCHQ in advance of the factors relevant to the grant of permission and any self-imposed limits, such as a ban on assassination, then, arguably, this would constitute a *policy*. If, however, there was no prior position but a request to authorise assassination of known terrorists had been refused, then it could be argued to constitute an *operational* matter. The practical result in terms of the service's actions might be identical, but in the first situation the Committee would be competent to investigate whereas in the second it would not. Similar points could be made about virtually any technique employed by the agencies, whether of recruitment, surveillance, agent handling, information gathering or disclosure.

The policy/operations distinction is reflected in the powers of the Committee. The agency heads may refuse to disclose what is described as 'sensitive information'.[10] This is defined in the Act to include information that might lead to the identification of sources, other forms of assistance given to the agencies, or operational methods. A second category of 'sensitive information' concerns past, present, or future specific operations. Within these categories refusal is *discretionary*. The head of one of the three agencies may disclose the information if satisfied that it is safe to do so (ISA, schedule 3, paragraph 3(2)). Moreover, the responsible Minister may order disclosure to the Committee the public interest notwithstanding (ISA, schedule 3, paragraph 3(3)), so over-ruling the agency head concerned. From a certain point of view, however, the status of the Committee's requests for information is enhanced since the demands that it makes have statutory backing, unlike those of a conventional parliamentary select committee.

10. ISA, schedule 3, paragraph 4. In addition, ministers have power to withhold 'non-sensitive' materials on grounds similar to those that apply to select committees: ISA, schedule 3, para. 3(4).

Some shortcomings in the Committee's brief can be noted. Unlike the United States, there is no tradition in the United Kingdom of confirmation by the legislature of the appointment of key officials. The executive alone is responsible. Consequently, the appointments of heads of the agencies are made by Ministers (presumably advised by the head of the civil service, the Cabinet Secretary) but without reference to the Committee's members. This gap became apparent with the political controversy in May 2004 surrounding the appointment of John Scarlett as 'C' (the head of SIS) (*BBC News*, 2004a); Scarlett was the Chairman of the Joint Intelligence Committee (JIC) and a central figure in the controversy over the public use of intelligence in the Iraq war then still under investigation by the Butler review. When it reported two months later the Butler review apparently felt that Scarlett's position had been undermined and that it was necessary to endorse his new appointment, notwithstanding its published criticisms. [11]

There are limits also to the Committee's information-gathering powers that are not obvious at a first glance at the Act. It may request 'information'. It does not have, however, power to demand particular *documents*, even those referring to the policy, administration or expenditure of the agencies. The difference became crucial in one investigation into the handling of the Mitrokhin archive: it was only under pressure from Ministers (who had asked the Committee to investigate in the first place) that the agencies agreed to hand over documents as such, rather than summaries. Moreover, there is no right to see officials from the security and intelligence agencies at a level lower than the Director or Director-General.

The Committee is required by law to produce at minimum an annual report, which is delivered to the Prime Minister and, thereafter, published, with any deletions agreed to on security grounds (ISA, s. 10(6) and (7)). The Prime Minister again has several levers in this process, including the timing of publication, being effectively with him rather than the Committee. In practice, the impact of the report can be diluted by publishing the government's response at the same time. A manipulative Prime Minister could use the control over timing to publish the report when public attention is distracted by other, more pressing, concerns. Significantly, the Committee has complained of unnecessary delay in publishing some of its findings (ISC, 2000, para. 103). Moreover, in the event of disagreement between the Committee and the Prime Minister over material to be deleted from the report, the latter can insist, although to do so would probably be counterproductive if it led to public dissent from the members of the Committee.

### *The Membership of the Committee*

Although the legislation was passed in 1994, the Committee did not come into operation until the following year and it had little opportunity to embark on a substantive programme of work before the 1997 election. It produced one brief report only (*Report on the Security Service's Work Against Organised Crime*, ISC 1996). However, much more important has been the Committee's work since 1997 and, of

11. *Report of a Committee of Privy Counsellors*, 2004, para. 39. Two members of the ISC (including the chairman, Ann Taylor) were members of the Butler review.

course, in the 2001–2005 parliament following 9/11. It is significant also that, unlike the previous administration, from the start of the new Blair government Ministers were accustomed to sharing oversight of the services with the newly-established Committee.

The membership of the Committee remained nearly constant for the duration of the 1997–2001 parliament and was an intriguing mixture of parliamentarians. Eight of the nine members were from the House of Commons – the sole peer was a former Labour Solicitor-General Law Officer, Lord Archer of Sandwell. The Committee was chaired by an experienced Conservative Member of Parliament, Tom King, who had substantial security and defence experience from time spent as secretary of state for Northern Ireland and Minister of Defence. Another member of the Committee, also Conservative, Michael Mates, MP, had a military background and had been a junior Defence Minister. Equally, though, the Committee included one Labour MP, Dale Campbell-Savours, who had taken a close interest in security matters as an outsider and had been a prominent critic of the lack of accountability of the services (and of the new legislative arrangements). Also highly experienced was Alan Beith, MP, the Deputy Leader of Liberal Democrats – the political party which had championed parliamentary accountability for security and intelligence agencies earlier than any other. At the other end of the experience range was Yvette Cooper, a new Labour MP with no previous experience of government or parliamentary committees and one of the youngest parliamentarians from the 1997 intake. To all appearances the Committee had been constructed to work in a bipartisan fashion, in view of the fact that it was chaired by a prominent member of the parliamentary opposition, and to be representative of a range of different parliamentary interests, including those highly sceptical of the entire process.

The Committee was reconstituted after the 2001 election due largely to individuals leaving parliament, although four of the nine members from the previous parliament remained. Tom King had retired and was replaced in the chair by Ann Taylor, a Labour MP who was a former Chief Whip (the senior government business manager in the House of Commons in effect). This cannot be seen as in any way sinister, however. The previous chairman was a Conservative who had been appointed by a Conservative Prime Minister and who was retained when Labour came to power. It cannot be said therefore that there was an established convention that the Committee be chaired by an opposition back-bencher, although that would clearly be helpful in maintaining a bipartisan approach to security matters.

At the 2005 election Ann Taylor retired from the House of Commons and the ISC was again reconstituted under a new chairman, Paul Murphy – a Labour MP and, like Tom King, a former Northern Ireland Minister. Any suggestion of an emerging convention that the chairmanship would rotate between government and opposition was thereby dispelled. In fairness, however, opposition MPs with intelligence experience were rare after 8 years of Labour rule (except serving members of the ISC itself). Perhaps also the greater prominence of intelligence since 2001 had made this Committee too politically sensitive for the Prime Minister to entrust to an opposition chairman. Although Paul Murphy and several

of the other members are new to the ISC,[12] there is some continuity: James Arbuthnot served on the committee in the 2001–2005 parliament and Alan Beith and Michael Mates remain from the original membership.

*The Committee in Operation*

The Committee's working method was to begin by familiarising itself with the agencies by meeting heads of the services and by visiting the various premises in which MI5, MI6 and GCHQ are housed. They seem to have encountered little resistance from officials who were, if anything, keen to establish a new source of legitimacy for their work with a committee representative of parliament rather than just government. It is perhaps significant also that the services themselves were in a transitional period both following the ending of the Cold War and the transition to peace in Northern Ireland. In this context no doubt the Committee could be seen as a useful ally in battles within government over budget priorities at a time when there was a risk of cut-backs due to the changing political situation. In any event good working relationships seem to have been established quickly.

From the start the Committee has been proactive. In an early report it warned that it expected to be 'properly and promptly informed' by the agencies of their activities, rather than merely responding to requests for information; in this the Committee was consciously following the Congressional oversight model, rather than the more responsive mode contemplated in the legislation (ISC, 1996, para. 37). It publishes an annual programme of work which it follows from year to year, as well considering topics which may emerge between annual reports in ad hoc reports. It has tended to meet frequently (often weekly during the parliamentary session). Typically it interviews several dozen witnesses each year, and takes part in international liaison and exchanges, both by visiting oversight agencies abroad and receiving such visits (these have included many European and former Soviet bloc countries, the US and the other Commonwealth states).

A key issue in the development of the Committee's work was the acquisition of a proactive investigative capacity. Without this facility the Committee would be able to hear evidence from witnesses but have no way in which to dig deeper into the performance of the agencies. The 1994 Act made no provision for investigations of this kind, whether by the Committee or any independent official, such as an Inspector-General. It might be argued that in view of the Committee's limited remit, investigation as such was unnecessary since it would venture into operational matters.

Nevertheless, the Committee argued that, compared to the oversight arrangement in other countries, it lacked the direct ability to investigate the agencies activities. Although generally satisfied with the level of cooperation that it had received in requests for access to information, the Committee argued that a power of

12. The membership at January 2006 was: Rt Hon Paul Murphy MP (chair), Ben Chapman MP, Rt Hon George Howarth MP, Dari Taylor MP, Baroness Meta Ramsay of Cartvale, Rt Hon Michael Mates MP, Rt Hon Michael Ancram, QC MP, Richard Ottaway MP, Rt Hon Alan Beith MP.

independent verification would give added authority to its findings and so strengthen public confidence in the oversight system (ISC, 1998, paras 67–9). The government conceded the issue without making a formal change to the powers of the Committee (Prime Minister, 1998, para. 21). The result then was a compromise in that the Committee stopped short of calling for the creation of an independent statutory investigator, such as an Inspector-General, but the government agreed that the agencies would cooperate with an Investigator working for the Committee. A retired Deputy Chief of Defence Intelligence (ISC, 1999, para. 84) was appointed to this role part-time. Defence intelligence is not within the Committee's statutory remit and, thus, the Committee was able to appoint someone with intelligence expertise but without loyalty to one of the agencies overseen under the Act.

The Investigator was 'tasked' by the Committee as part of its annual programme of work to investigate and report to it on certain topics. Thus, for example, in 2001–2002 the Investigator was asked to investigate scientific and technical research and development supported by the agencies, how the roles discharged by Inspectors-General in other countries were met in the UK, recruitment, retention and career development in the agencies, and to review the US Report 'A Review of FBI Security Programs' (ISC, 2002a, paras 93 ff).

The use of the Investigator came to an abrupt end in July 2004 when, nearing the end of his five-year term, the incumbent, John Morrison, gave an extended interview to the BBC's *Panorama* programme relating to his previous responsibilities as Deputy Chief of the Defence Intelligence Staff (DIS). In it he catalogued political intervention in intelligence analysis and criticised the Prime Minister's repeated claim that intelligence had shown that Iraq was a 'threat' to the UK. On his own account Morrison was then told by the ISC Chairman, Ann Taylor, that his contract would not be renewed because the agencies had indicated that they could no longer have trust in their dealings with him (*BBC News*, 29 October 2004b). In view of the very specific matters publicly raised by Morrison and the nature of his later duties this is hardly surprising, whatever the merit of his allegations. Clearly he would have been a candidate for prosecution under section 1 of the Official Secrets Act 1989, although, as in the case of Katherine Gun, that would have only served to give him a further platform from which to highlight uncomfortable allegations about Iraq. Perhaps more unfortunate was the statement by an unnamed spokeswoman that the ISC did not intend to appoint another investigator. Morison's behaviour was treated with studied disdain: the 2004–2005 ISC Annual Report echoes with a deafening silence on the whole episode, mentioning neither him nor the office of Investigator, as though he was one of the 'disappeared' and the role had not existed for part of the year under review. This is unfortunate. The issue of whether the use of an Investigator is a worthwhile innovation deserves discussion on its merits and should not be foreclosed by the response to an isolated abuse. In an earlier report the Committee concluded:

> The addition of an Investigator has allowed us to pursue issues in greater depth than if we had to rely on out efforts and resources. While the Investigator does not have an IG's powers, in practice the Agencies have proved most cooperative; the knowledge that they can call for operationally sensitive material to be removed from

> the Investigator's report before it goes to the Committee report encourage them to be frank (ISC, 1999, para. 85).

This comment perhaps captures the sense of pragmatic compromise in these arrangements. From a rigorous democratic perspective, however, this was oversight by licence, rather than as of right. John Morrison's dismissal at the request of the services demonstrates this clearly. If anything, this brief experiment perhaps shows what the addition of a statutory Inspector-General might bring to the UK arrangements.

Apart from the depth of its investigations, it is clear that the Committee has worked well beyond its strict legal remit in terms of agencies overseen also. The ISC has encountered no apparent opposition in investigating the work of the Joint Intelligence Committee and the Intelligence Coordinator, parts of the intelligence machinery which although closely linked to the agencies are outside the statutory framework (ISC, 1999, paras 8 ff). Similarly, it has taken evidence from a number of government departments which are in effect the security and intelligence agencies' 'customers', which are the users of intelligence produced by them or suppliers, including the Defence Intelligence Staff and police Special Branches.

An example that shows the ability of the Committee to conduct an in-depth and independent investigation is the report on intelligence and threat warnings preceding the Bali bombing of 12 October 2002 (*The Times*, October 13, 2002. ISC, 2002b). On the face of it the report went considerably beyond the statutory remit of the Committee, since it concerned specific intelligence available in relation to a specific event. Moreover, in the conduct of its inquiry the Committee examined all the relevant intelligence, intelligence assessments and travel advice available before the attack – in other words, it was given access to intelligence files as well as interviewing witnesses. The explanation is that the initiative for the inquiry seems to have come either wholly or in part from the government itself, which wanted to be able to substantiate the claim that no specific warning of a threat had been received which should have been made public. To make this claim credible it was necessary for it to be investigated by an independent body. Hence, it was the Foreign Secretary who announced to the House of Commons that the Committee was conducting an inquiry and that all material would be made available to it (HC Debs., 21 October 2002, cols. 21–24). Nevertheless, the ISC produced an independent report sharply critical of the Security Service (the agency responsible for formulating and distributing terrorist threat assessments). It exonerated officials from the claim that there had been specific information of the attacks that had not been passed on. It concluded authoritatively that there had been no such information and, therefore, the attack could not have been prevented. However, it found that the Security Service had been guilty of a 'serious misjudgement' in failing to issue a higher level of threat warning.

There are, though, some glaring omissions from the published work of the Committee. Foremost among these is the silence on the allegations of the former Security Service officer David Shayler, finally convicted in 2001 under the Official

Secrets Act for his revelations concerning the agency,[13] and his counterpart from MI6, Richard Tomlinson. The allegations of incompetence and abuse made by these two insiders have received no public investigation. The reason is apparently that the Committee did not wish to encourage 'whistle-blowers' who break the law. Instead, the Committee has taken a close interest in the personnel policies of the agencies. The unstated implication was that these cases are instructive only because of the failure to handle them in-house, rather than because of the substance of the allegations. And yet if the Committee is prepared to listen only to officially-sanctioned evidence, it is arguably depriving itself of a valuable source of information.

In the later similar case of Katherine Gun, the ISC was more visibly engaged, although still not to the extent of interviewing the former official herself. In February 2004, proceedings brought under the Official Secrets Act 1989 against Katherine Gun, a translator formerly employed as a linguist at GCHQ, were dropped without explanation (*BBC News*, 2004c). She had disclosed a request from the US authorities to intercept communications of other countries voting on action against Iraq at the United Nations. The ISC in effect confirmed the government's contention that the decision to offer no evidence against Gun was not, as many newspapers alleged, because the trial would have brought embarrassing disclosures about the legality of the war (ISC, 2003c, para.72). The Committee hinted without explaining that an unspecified misunderstanding between the prosecution and GCHQ had been to blame. The suggestion of a cross-agency legal review that it proposed to prevent similar mistakes was, however, rejected in the government's response. On this occasion ISC suggested that a review of the Official Secrets Act was necessary (ISC, 2003c, para. 92*;* ISC, 2004, para. 150) in part because of concerns from whistle-blowing cases. Some of its comments suggest, however, that it would favour a tightening of the law rather than the creation of a public interest test of disclosure (ISC, 2004, para. 151).

Among the concerns that the Committee has expressed in its reports is a recurring argument that Ministers should be more directly involved in overseeing decisions of the agencies. This theme has surfaced in a variety of contexts.

In its annual reports, the Committee has repeatedly drawn attention to the inactivity of the Ministerial Committee on the Intelligence Services, which in theory looks at the policy of the agencies, together by approving annual budgets and the intelligence Priorities and Requirements, under the Prime Minister's chairmanship (ISC, 2000a, para. 19). In practice, the Ministerial Committee seems to be moribund (it had not met since 1995 prior to its 2003 meeting). The government's response was that there is little point in the Ministerial Committee meeting merely for the sake of doing so and that the Committee would be convened if there were substantive business to discuss. A government undertaking

13. See Machin, 2005. The author (the girlfriend of Shayler) is herself a former MI5 officer.

that the Ministerial Committee would meet at least annually in the future[14] was broken almost immediately (ISC, 2005, para. 14). The Committee's criticism that Ministers meet intelligence officials primarily in the context of a crisis or single issue meetings rather than to discuss collectively intelligence requirements and developments looks well taken. If correct this means that there is a significant gap in oversight.

A series of recommendations in recent reports suggests that the ISC is increasingly troubled by the agencies' failure to brief Ministers adequately or promptly on some matters. As part of its investigation into the agencies' role in handling information from the KGB defector, Vasili Mitrokhin, the Committee examined decisions not to prosecute spies in UK public bodies who had been exposed as a result (ISC, 2000b; PM, 2000a). One of these cases, that of Melita Norwood, came to prominence mainly because the press were fascinated by the possibility that an 87-year-old grandmother might be prosecuted for espionage relating to her activities going back to the 1930s. The Committee's concern was that Ministers had not been properly informed of her case so that when the Attorney-General first heard of it in 1999, prosecution was in effect barred by lapse of time. Nor had successive Ministers been properly briefed by officials over (the MI6-sponsored) plans to publish material derived from Mitrokhin.

One might have thought that, after 9/11, Ministers would be proactively involved in intelligence and security policy. However, the ISC has drawn attention to delay in sending Ministers the *Annual Review of the JIC Chairman* (ISC, 2005b, para. 19) – in view of the current prominence of intelligence on the political agenda. A review of previous performance is of crucial salience in future planning. Equally sensitive is the recent recommendation that Ministers should be 'informed *forthwith*' if intelligence reports on which they had been briefed are withdrawn (as had happened with several important reports concerning alleged Iraqi weapons of mass destruction).[15] Finally, the Committee's report into interviewing of detainees in Afghanistan, Guatanamo Bay and Iraq found that Ministers should have been consulted before staff from the agencies had interviewed captives in the hands of the US military in Afghanistan and that Ministers should be informed 'immediately' when an official has concerns about the treatment of such detainees (ISC, 2005a). Against the background of mistreatment and alleged torture of some of these detainees, the significance of these recommendations is self-evident.

There have been a number of issues on which the ISC and the government have engaged in low-level skirmishes, with honours fairly evenly divided. Pressure from the Committee persuaded the government to reconsider the proposed arrangements and to introduce an independent element into the disposal of security files from the Cold War period – a valuable historical resource (HC Debs. vol. 318, col. 649–650, 3 Nov. 1998; ISC, 1999, paras. 76 ff). However the government has refused to give

14. Prime Minister, 2000b. ISC, 2002a, para. 10 expressed continued concern that a formal meeting had still not been convened, although the same group of ministers had met regularly with security officials regularly post 9/11.
15. ISC, 2005b, para. 63, emphasis added (remarkably the ISC were told by MI6 of the withdrawal of some reports before the Foreign Secretary).

way in a long-running disagreement over whether the publication of budgets for the individual agencies, rather than a total 'Single Intelligence Vote' is sensitive. After protest at the government's continued intransigence (ISC, 2001, para. 26), the Committee seems to have given up on the issue. Similarly, the Committee has consistently argued that in order to perform its role it requires access in full (rather than to the edited, published version) of the reports of the Commissioners who check the legality of ministerial warrants under the 1994 Act and for interception of communications (where requests can be made by the Services). The government has opposed this in principle, although it has indicated that it is prepared to discuss specific requests. As a compromise, the Committee has met with the judicial Commissioners but it still maintains that it needs to see the reports in full (ISC, 2002a, paras. 29 ff). Despite the lack of information, the Committee has not felt inhibited from investigating and commenting on the possible use of intercept evidence in criminal trials (ISC, 2005b, paras. 92–94).

An assessment of the Committee's work would not be complete without reference to one final matter that has thrust it from relative obscurity into fiercely politically contested territory – Iraq.

*The Committee's Report on Iraq*

Inevitably, the Committee has taken a keen interest on the use of intelligence prior to the 2003 war in Iraq, amid claims that it had been politicised. The UK government chose, in the attempt to enlist public and political support for its policy, to release two dossiers of intelligence-related material concerning the attempts of the Iraqi regime to acquire and develop 'Weapons of Mass Destruction' in September 2002 and February 2003. According to press reports, the intelligence agencies had misgivings about the publication of material in this way (subsequent evidence of the Hutton Inquiry[16] highlighted concerns within the DIS. Whether for that reason or some other cause, the second dossier was based in part on 'open source' material, rather than intelligence assessments from the JIC. This proved a catastrophic mistake, when large parts of the 'dossier' (which became christened 'the Dodgy Dossier') were found to have been plagiarised from a PhD thesis written 11 years earlier. The Intelligence and Security Committee later commented that it supported 'the responsible use of intelligence and material collected by the Agencies to inform the public on matters such as these' but that it was 'imperative that the Agencies are consulted before any of their material is published'. It noted that this process was not followed in relation to the February 2003 dossier:

16. The judicial inquiry under Lord Hutton appointed to investigate the events surrounding the death, in July 2003 of Dr David Kelly, an expert working for the Ministry of Defence. Dr Kelly had been publicly identified in controversial circumstances as a possible source for a BBC news story that the dossier had been altered. He was found dead having previously given evidence to the ISC (in private) and televised testimony to the Foreign Affairs Select Committee, Hutton, 2004.

> Although the document did contain some intelligence-derived material it was not clearly attributed or highlighted amongst the other material, nor was it checked with the Agency providing the intelligence or cleared by the JIC prior to publication (ISC, 2003a).

The allegation that the intelligence dossiers were altered under political pressure prior to publication in order to make the case for war appear stronger was central to a subsequent investigation by the Committee.[17] In a high profile investigation the Committee interviewed the Prime Minister, his controversial press secretary (since resigned) Alistair Campbell, and other senior Ministers, including the Defence Minister, Geoff Hoon. It also saw the entire text of successive drafts of the published intelligence dossiers and was able to track the changes made and the reasons for them. The Committee's report rejected the allegation that the dossiers had been doctored for political purposes. It did however criticise the prominence given to one claim (that Saddam Hussein possessed weapons of mass destruction that could be brought into use in 45 minutes) and the partial and misleading treatment given to it.[18] The Defence Minister, Geoff Hoon, was singled out for having been uncooperative in trying to conceal misgivings within his own department (ISC, 2003b, Paragraphs 104 and 105). However, the report stopped short of accusing him of deliberately misleading the Committee.

By comparison with the Hutton inquiry, the ISC appeared somewhat unglamorous. Unlike Hutton, it examined witnesses in private. There was no public cross-examination of officials and Ministers by lawyers. Although reports of Hutton's hearings dominated the news during July and August 2003 and made the legal personnel involved into minor celebrities, their value perhaps lay more as an exercise in public accountability rather than in eliciting information. Unquestionably some of the witnesses (Ministers particularly) postured before the inquiry and, although the experience of cross-examination may have been unsettling, they emerged essentially unscathed. Moreover, like the ISC before it, the Hutton report exonerated the government (Hutton, 2004). The Hutton report did, however, perform a valuable service in publishing much documentary material – ironically a good deal of it given to it by the Intelligence and Security Committee, but not published by it. That aspect suggests that the Committee could work substantially more openly without unduly compromising secret material.

Although couched in different language and containing an eye-catching criticism of the informal style of decision-making in the Blair administration, the report of the Butler committee (Butler, 2004) did not differ from the ISC (or Hutton) on the core question of whether the publicly-presented intelligence on Iraq had been tampered with for political reasons. The report went further in proposing safeguards over future public uses of intelligence and in suggesting changes in MI6, Defence Intelligence and JIC practice. Some of these matters were outside the

17. ISC, 2003b. The House of Commons approved a motion on 16 July 2003 (by then the ISC's investigation was already underway) affirming that it believed the ISC was the appropriate body to investigate claims relating to intelligence and Iraq.
18. 'The omission of the context and assessment allowed speculation as to its exact meaning. This was unhelpful to an understanding of this issue' (ISC, 2003b, para. 86).

terms of reference of the ISC's initial investigation but, in any event, they have been taken up by it in monitoring the agencies' implementation of Butler.

Whether the ISC is less effective than other investigatory devices is questionable. Some commentators have used the Iraq experience to compare it unfavourably with the Hutton Inquiry or the Butler committee review.[19] However, this downplays the exceptional nature of judicial inquiries and committees of Privy Counsellors, which have added legitimacy in part because they are used more sparingly than parliamentary committees. Satisfying as the public spectacle of cross-examination before a Law Lord may seem, it is unclear that in practice it brings to light qualitatively different evidence. Equally much of the praise heaped on the Butler review neglects the point that it was not a one-man investigation (Lord Butler was a former Head of the Civil Service) but an investigation by a *committee*. Two of the five members (Ann Taylor and Michael Mates) were in fact members of the ISC and it would be surprising if the Butler investigation did not owe a great deal to their prior familiarity with the same material. The ten-month time difference between the ISC and Butler reports also accounts for some of the additional material solicited (especially information about the later withdrawal of intelligence by MI6).

The ISC certainly compares unfavourably in terms of resources to either a judicial inquiry or, for that matter, a congressional committee. Peter Gill has noted the entirely different scale of the US investigations (with 24 researchers employed by the Joint Inquiry team and 300 witnesses interviewed, compared with the 37 witnesses interviewed by the ISC) (Gill, 2004, pp. 467, 484–5). However, much the same point could be made comparing any congressional committee with any parliamentary committee: it reflects broader constitutional differences, rather than a specific problem with the ISC. On the other hand, Philip Davies has argued that despite the different scale of the US post-Iraq investigations, the ISC succeeded in securing access to some better information (notably the Joint Intelligence Committee assessments on Iraq up to March 2003) (Davies, 2004, pp. 495, 511).

## Conclusion

Generally speaking, the Intelligence and Security Committee can be counted a success on several levels.

Firstly, at a presentational level, the existence of the Committee has largely assuaged calls for more public accountability of the security and intelligence agencies. It is true that there remains the constitutional objection that the Committee is not responsible to parliament as such. For this reason, the Home Affairs Committee has continued to call for the Intelligence and Security Committee to be replaced with a Parliamentary Select Committee (UK Home Affairs Select Committee, 1999). However, even it has conceded that the existing

19. Danchev, 2004, p. 436. On the Iraq inquiries see also: Glees, 2004, p. 138; Phythian, 2005, p. 124; Gill, 2005.

Committee is a significant improvement on the previous arrangements and has paid tribute to its work.

Secondly, the Committee has plainly succeeded in establishing good working relations with the security and intelligence agencies. The only clear indications of friction have been in relation to the Committee's investigation into intelligence before the Iraq war. The Committee's rebuke of the Ministry of Defence for failing to make clear internal disagreements has been noted earlier. It subsequently became clear also that, despite contrary assurances, the ISC had not been shown all relevant JIC assessments on Iraqi weapons of mass destruction and on Iraq generally. Although attributing this to a mistake rather than an attempt to mislead, and stating that the relevant documents did not affect its conclusions, the ISC nevertheless expressed 'considerable concern' (ISC, 2004, para. 145). If anything this is a masterly understatement: it is frankly astonishing that in an investigation of this sensitivity and importance that such material was overlooked by officials.

It is significant, perhaps, that the government evidently trusted the Committee sufficiently to ask it to investigate two matters which involved access to considerable *operational* detail (and which were therefore well outside the Committee's statutory powers) – the handling of the Mitrokhin Archive and intelligence prior to the Bali bombing. The same is true of the investigations that the ISC initiated into intelligence prior to the Gulf War and the involvement of UK personnel in the treatment of detainees held by the United States. Moreover, the Committee has succeeded in behaving in a non-political fashion so that its criticisms of the agencies have generally been responded to in a constructive fashion.

Thirdly, the Committee has worked well despite its relatively weak powers. As has been pointed out above the Committee has only weak legal entitlements to information and none to documents as such. Nevertheless this does not seem to have been an insuperable difficulty. This may be in part because the agencies were aware that withholding information in accordance with the strict terms of the Act would inevitably have produced public and parliamentary calls for increased investigative powers.

Moreover, in some cases for the government to have asserted its legal rights and thereby refuse access to documents would have been politically inept. To do so would have undermined the credibility of the Committee's investigation and hence resulted in increased criticism of the government. However, this is not to suggest that the government has co-opted the Committee to its cause: there is no evidence of anything other than thorough and independent investigative work, together with balanced and, where the evidence supports it, critical reporting. The most that can be said is that government and the agencies have an interest in the Committee being seen to operate independently and effectively, and, knowing this, the Committee can exert its own pressure to obtain cooperation.

Perhaps two positive steps could be taken to dispel the residual nagging doubt that the ISC's relationship to the agencies is a little too close. Firstly, the Committee could do more to take evidence from outside the ring of secrecy, especially on policy matters where outsiders may offer informed alternative

perspectives. For the most part the Committee has heard evidence only from serving intelligence officers, although a recent exception was the evidence taken from newspapers over their liaison with the agencies (ISC, 2005b, paras 80–88).

Secondly, a more robust attitude might be taken to the publication of information. The Committee's reports contain many deleted passages where excisions have either been negotiated or insisted upon by the Prime Minister, (although, apparently, never against the outright wishes of the ISC). It is questionable whether this is always necessary in the light of the publication of much unexpurgated intelligence material by the Hutton inquiry and the Butler committee. At a press conference Lord Butler pointedly commented that *his* report had 'no asterisks' (that is, deleted passages). The UK Intelligence and Security Committee's reports sometimes leave a reassuring feeling that the Committee has been active but without its full findings and recommendations being published. This, however, is the recurrent difficulty of oversight – how to reconcile effectiveness with giving a public account.[20]

20. Two further valuable sources became available after completion of work on this chapter: ISC, 2006 and Glees, Davies and Morrison, 2006.

Chapter 12

# Democratic and Parliamentary Accountability of Intelligence Services After 9/11

*Peter Gill*

## Introduction: The Need for Democratic Accountability[1]

In the past 30 years throughout Europe, the Americas and more sporadically elsewhere, the issue of how to institute some democratic control over security intelligence agencies has steadily permeated the political agenda. There have been two main reasons for this change. In what might be described as the 'old' democracies (those of North America, Western Europe, Australia and New Zealand) the main impetus for change was scandals involving abuses of power and rights by intelligence agencies. Typically, these gave rise to legislative or judicial inquiries that resulted in new legal and oversight structures for the agencies, some of these achieved by statutes, others by executive order. The best known examples are the US congressional inquiries during 1975–1976 (chaired by Senator Church and Representative Pike), Justice McDonald's inquiry into the Royal Canadian Mounted Police (RCMP) Security Service in Canada (1977–1981) and Justice Hope's inquiry into the Australian Security Intelligence Organisation (1976–1977, 1984–1985).

Elsewhere, this shift has been a central, and sometimes painful, aspect of the democratisation of formerly authoritarian regimes, both civilian and military. For example, the death of Franco in 1976 precipitated democratisation in Spain that included the demilitarisation of intelligence (Giménez-Salinas, 2003). Military rule ended in Brazil in 1985, though the military dominated National Intelligence Service (SNI) was not replaced until 1990 as part of a continuing process of demilitarisation (Cepik & Antunes, 2001). During 1993–1994 a more rapid transformation of formerly repressive security agencies was attempted in South Africa (Joffe, 1999). The other major examples of this transition since 1989 are the countries of the former Soviet bloc where no agency has been immune to the changes although the amount of real, as opposed to nominal, reform varies widely (for example, Rzeplinski, 2003; Szikinger, 2003).

1. This chapter deals with the period until June 2005.

Whether scandal or the democratisation of former authoritarian regimes (and sometimes both together) have been the impetus for change, the main emphasis of reform has been on increasing the legality and propriety of security intelligence operations. Although in some cases attention was also paid to the issue of achieving effective security intelligence (for example, McDonald, 1981), the overall direction of change was for the better control and accountability of agencies whose past activities had been dominated by the surveillance of political opponents rather than genuine security threats.

But since the 9/11 attacks in New York and Washington DC, the debates around security intelligence have shifted to contemplation of 'intelligence failure' and the question of how future threats can be averted. This is most obviously the case in the US itself, although the impact of the global 'war on terror' has been much more general. This repeats the historical pattern in which concern regarding propriety has increased following scandals, while intelligence 'failures', such as 9/11, give rise to an increased concern with efficacy. In this atmosphere it is easy to see how the democratic gains of the last thirty years might be swept away in the naïve belief that the agencies 'unhampered' by oversight requirements might somehow be more efficient and effective.

It is a mistake to view efficacy and propriety as being in a zero (constant) sum relationship such that gains in one are balanced by losses in the other. Rather, they should be viewed as being in a non-zero (variable) sum relationship such that both can be improved. This is not to say that there is no tension between the two: it is quite easy to see how, in the short run, the ability to conduct surveillance of an individual or group may be reduced by the requirement to follow procedures that seek to protect privacy but, in the longer term, such procedures are required if a state is to be entitled to call itself democratic. Such procedures should be designed to ensure that, even in the short term, the invasion of privacy is proportionate to the alleged threat, but also to prevent it from being directed at the wrong person or conducted in such a way as to amount to intimidation. Thus legal rules themselves may contribute to efficacy as much as to propriety.

In the search for better public control of intelligence, improved legal rules alone will be insufficient. The task of democratisation and the search for efficacy/propriety includes shifting both the legal context for intelligence work and the *culture* of the agencies. Although the process of achieving legislative change can itself be difficult and requires considerable political will, there is a danger that, once it is achieved, it will be assumed that real change in the agencies and their behaviour will automatically result. This is a dangerous assumption: new laws themselves may only achieve symbolic change (Edelman, 1964), so that the public can be reassured that problems have been dealt with. However, if they are not matched by even greater effort in implementing those laws then little in reality may change. Beneath the surface of new laws, what the agencies actually do and how they do it might remain essentially unchanged. Achieving cultural change in agencies with histories of considerable autonomy from outside control or influence is a long term project that requires even greater political will than achieving initial legal reform.

It is important to define some key terms. 'Control' is relatively straightforward: it refers to the management and direction of an organisation and can be exercised at various levels; for example, if a parliament passes a law relating to the mandate and operations of an agency, then we can justifiably talk of 'statutory control'. Closer to the agency, we might talk of 'executive' or 'political' control where a member of a government (such as an Interior Minister or Attorney General) may issue directives to an agency. Then, within the agency itself we might talk of administrative control by a Director including the promulgation of internal regulations and guidelines.

'Oversight' is often used interchangeably with 'review'. This may be because in some languages the terms are interchangeable; for example, in the French version of the Canadian Security Intelligence Services Act 1984, the term *surveiller* is used to describe what is described in the English version as 'review'. In early days of the Act there was some controversy surrounding the role of the Security Intelligence Review Committee (SIRC – see below). Critics of its activism argued that 'review' was a *post hoc* activity whereas those advocating a more extensive role including, if appropriate, ongoing operations preferred to rely on *surveiller*. Thus the interchangeability of the terms can disguise what is actually an important distinction. For the purposes of this discussion it is useful to adopt Caparini's definition: to use review to describe an *ex post facto* process and oversight to describe a process of supervision that might include ongoing activities (Caparini, 2002, p. 5).

## Some Principles of Control and Oversight

Much can be gained from the comparative study of security intelligence (Hastedt, 1991). The use of security intelligence by states displays certain common features regardless of their precise form – for example, secrecy, a tendency to confuse 'security threats' with 'political opposition' and the use of 'extra-legal' methods to obtain information and disrupt opponents. Also, it is possible to see the development of cross-national intelligence 'communities' or networks so that the differences between national agencies may be less than assumed. To be sure, this tendency is clearest within coalitions of nations, for example, the United Kingdom-United States of America (UK-USA) pact of Anglo-Saxon countries, especially their signal intelligence (SIGINT) agencies, or the Warsaw Pact between what were 'counterintelligence states' in Eastern Europe. Elsewhere, and sometimes even within coalitions, there are fierce 'intelligence wars' between agencies but there are now clear signs of convergence between agencies in the context of the globalised 'war on terror' led by the hegemonic United States.

Even a cursory examination of developments in different countries during recent decades indicates that there is no single 'rulebook' for the design of architectures of democratic control and oversight or review (cf. Born and Leigh, 2005). Clearly, the sets of legal and institutional relationships that emerge in any specific country will be the product of its unique culture, history and politics. Thus, any comparative enterprise such as that providing the inspiration for this project

must start with respect for these varying traditions. Since political institutions cannot simply be transplanted from one political system to another, it is idle to suggest that states might simply pick and choose from institutions operating elsewhere. However, there is no point in a comparative analysis if the only objective is to provide an exhaustive description of the variety of practices. If academic social science is to contribute anything to a debate that concerns most directly intelligence and political professionals, but has repercussions for the quality of democracy, then it must be to analyse the governance of intelligence so that the specifics of debates everywhere are informed. Studying institutions elsewhere may well help to prevent a state from 'reinventing the wheel' – states can learn from each other. For example, in the wake of the Bali bombing in October 2002, the UK Intelligence and Security Committee (ISC) was critical of the then threat assessment system located in the Security Service's Counter Terrorism Analysis Centre, which had only just started operating (ISC, 2002b). Consequently, the Security Service developed a Joint Terrorism Analysis Centre (JTAC) to which all the other main agencies and departments contributed personnel, each with access to their own databases. During this process, discussions were held with the similarly multi-agency US Terrorist Threat Integration Centre (TTIC – since reconstituted as the National Counterterrorism Center: NCTC) and with Israel, where experience with suicide bombings is greater.

Thus, in this chapter, the objective is not to lay down hard and fast rules for effective public control; rather, it is to suggest that there are certain fundamental questions that have to be answered and certain basic principles that can be enumerated based on the study of intelligence reform in several countries. Figure 12.1, 'Control and Oversight of Security Intelligence Agencies', summarises the key relationships. The horizontal axis is based on the proposition that 'states' are not single entities: they operate at three main levels, the demarcation between them often indicated by secrecy barriers. First, there is the most secret level occupied by security and military intelligence agencies; second, the executive branch (or government) and, third, the broader array of state institutions including elected assemblies, judiciaries and bureaucracies. Since we are concerned with the issue of public control, we must also include a fourth – non-state – level in our analysis, comprised of citizens, media, organised groups and social movements.

The vertical axis seeks to summarise, firstly, the different institutions and forms of control that need to exist at each level and, secondly, the complementary institutions of oversight or review. Forms of control become more specific the closer the level is to the agencies. The manifestos generated by political parties or social movements are not, strictly-speaking, a form of 'control' because they may have no impact on agencies but they will provide a general set of ideas that might at some point inform more specific statutes or court actions. Some parliaments pass more detailed legislation than others; but in either case Ministers are likely to provide yet more detailed directions for agencies. Some legislation actually requires Ministers to provide directions, for example, the CSIS Act. The most detailed rules or 'guidelines' will be those developed within the agencies that are normally unpublished.

**Figure 12.1 Control and Oversight of Security Intelligence Agencies**

| **Level of Control/ Oversight** | **1. Agencies** | **2. Executive branch** | **3. Other State Institutions** | **4. Citizens & Groups** |
|---|---|---|---|---|
| **Form of Control** | Guidelines | Ministerial Directions | Statutes, Cases | Manifestos |
| **drawn up by ...** | | | | |
| **Institutions of Control** | For example Director | For example Attorney General | Assemblies, Courts | Political parties, NGOs |
| **report to ...** | | | | |
| **Institutions of Oversight** | For example Professional Responsibility | For example Inspector General | For example Oversight Committees | Citizens, Media |

- - - - - - - Barriers of secrecy

*Source*: Adapted from Gill, 1994.

Clearly, the central institutions of control identified in Figure 12.1 also play a role in oversight. Indeed, in some parliamentary systems prior to intelligence reform, it was claimed that it was inherent in the constitutional process that there could be no independent oversight of security intelligence and that both control and oversight were provided by the doctrine of 'ministerial responsibility' to the parliament. Even though the inadequacy of this doctrine has now been acknowledged, we can see that Agency Directors, Ministers, parliaments and some judges will exercise both functions. This is inevitable but becomes a problem if there are no additional institutions of oversight with their own organisational foundation.

Independent oversight institutions must therefore also be located at each level and must report to those responsible for control at that level. Their location within agencies or ministries raises concerns as to the real extent of their independence although the danger of them being compromised can be reduced by securing their right to communicate with oversight bodies at other levels (see below). It may seem odd to talk of oversight functions within agencies themselves but if oversight is only an external function then it becomes easier for agencies to see it as something troublesome that should be resisted. Rather, ideas of propriety must be internalised within the culture of agencies. Therefore internal oversight is

a necessary condition for public control but it is not sufficient – it must be reinforced by external oversight at levels two and three.

At level three, the most systematic review or oversight is likely to be provided by specialist committees either inside national legislatures, for example, the Intelligence Committees of the US Senate and House of Representatives (for an overview see Holt, 2000), and the joint committees made up of members of both houses in the UK and Brazilian parliaments; or outside national legislatures, such as the SIRC in Canada and the Committee for Monitoring of Intelligence, Surveillance and Security Services in Norway. The other potential oversight institution at this level is the judges who, in some countries, are involved in the authorisation of warrants for intrusive surveillance (in terms of the earlier discussion of terminology, this role involves elements of both control and oversight). Also, more episodic reviews may be provided by the courts.

Oversight bodies are usually quite small and have limited resources. Their effectiveness can be enhanced in several ways, such as by seeking to protect their independence by requiring them to copy reports to the oversight body at the next level. Depending on the precise institutional arrangements, this may be subject to some secrecy constraints but it will help to reduce the dependence of oversight on the agencies themselves. If an internal agency body such as the 'Office of Professional Responsibility' reports to the Agency Director on some matter, the report should also be made available to whatever oversight institution exists within the ministry, for example, an inspector-general. Similarly, reports from inspectors-general to the Minister should be made available to the review committee at level three, whether it is a joint parliamentary committee such as in Brazil or the UK, or a non-parliamentary body such as SIRC in Canada. If reports cross the secrecy barriers existing between the different levels of the state (represented in Figure 12.1 by a broken line) then how is appropriate security of information to be maintained? Ultimately this has to rely on consultation and trust between institutions at different levels and the discretion exercised by those involved. This is particularly the case for those working at level three who, elected or not, must provide some accounting to citizens. Clearly, these people cannot simply reveal all they know to other parliamentarians or the public (hence the diagonal 'secrecy' line in Figure 12.1), but they must be prepared to lift the veil of secrecy and reveal what they discover unless it would clearly damage the security of the nation or the rights of individuals.

Secrecy is relevant to intelligence in two distinct dimensions: the first seeks to ensure that state officials will only have access to information if they have been cleared by security vetting for access at the appropriate level of classification. Normally, the higher an official is promoted or the nearer they are working to military or security matters, the higher the clearance they will need – for example, from 'confidential' to 'secret' to 'top secret'. Within the security intelligence sector, the second dimension is compartmentalisation. Even though officials may be cleared to the highest level, it is still believed that the circulation of knowledge with respect to particular techniques, operations or targets should be minimised in the interests of security. Therefore, individuals only have access to the information that they 'need to know'.

Now, these dimensions of secrecy have many implications. For example, they may hinder the efficacy of intelligence by reducing the flow of information both within agencies and, even more, among them. The failure of agencies to share information through some combination of proper concerns for security and petty bureaucratic jealousies is a common feature of intelligence 'systems'. The US inquiries into 9/11 identified the serious extent of this problem and argued that the 'need-to-know' be replaced by the 'need-to-share' (Kean & Hamilton, 2004, 13.3). Also, secrecy presents a major hurdle to be surmounted if public control is to be achieved. The ability of outside bodies to oversee or review intelligence agencies depends on their ability to obtain relevant information; if the agencies themselves do not provide it then those bodies will be obstructed because there will be little information available that is independent and useful. In most areas of state policy there is a broader 'policy community' of research organisations, 'think tanks', lobbying groups, journalists and academics who can provide a source of information and ideas independent of the state, but in the area of security intelligence this source is quite small. There have been numerous information and secrecy struggles between executive and oversight committees since 9/11, some of which are discussed below.

In general, it is most important that oversight institutions at different levels cooperate and help each other; this will not be without difficulty since the primary organisational loyalties of agency staff, inspectors-general and parliamentarians are very different, but without such cooperation oversight will be fragmented and consequently less effective. This becomes increasingly important because of what might be called the 'decompartmentalisation' of intelligence. For example in Europe (well before 9/11), a convergence of various issues was evident in what Bigo (1994) called the 'security continuum' (terrorism/drugs/organised crime/illegal immigrants/asylum seekers). 9/11 has reinforced this and we see it in institutional form in the similar convergence of what used to be relatively distinct fields of intelligence: military, foreign, domestic/internal, and law enforcement.

## Aspects of Control since 9/11

In order to provide an initial evaluation of the impact of 9/11 on the relative strengths of control and oversight, a brief discussion is proposed of some of the actions taken by executives, oversight committees, courts and judges. Most of the examples are taken from Canada, the US and the UK. Unsurprisingly, political executives responding to a perceived 'failure' on the scale of 9/11 will try to increase their capabilities for both a) action/power and b) information/intelligence. Changes have been made in each of the forms of control shown in Figure 12.1. New statutes were rapidly passed before the end of 2001 – in Canada the Anti-Terrorism Act, in the US the PATRIOT Act and in the UK the Anti-Terrorism, Crime and Security Act. Each of these extends the legal powers of governments to carry out surveillance and act against individuals and groups identified as terrorists and, in the case of the UK, engaged in other serious crimes.

But it is not just legal rules that have been rewritten; probably the most dramatic assertions of power have been those in the military field, especially the extension of the traditional right of national self-defence to encompass pre-emptive attacks, though these are beyond the scope of this paper. Whereas, in the wake of the intelligence scandals and inquiries of the 1970s, the US Congress sought to restrict the autonomy of the intelligence agencies (see for example Johnson, 1985; Olmsted, 1996), many of these restrictions are now being modified if not abandoned. For example, questions have been raised concerning the extent to which the expansion of US Special Forces operations overseas has been consistent with the statutory requirement for prior notice being given to the Intelligence Committees (Shanker and Risen, 2002). Another restriction was the erection of a 'firewall' between information generated for intelligence purposes and that used for the purposes of prosecution in the US. Since the 1970s, the increasing cooperation between military, intelligence and law enforcement agencies in the targeting of organised crime and the increased use of tactics of disruption (rather than arrest and prosecution) had already put pressure on this division. In the wake of 9/11, the firewall was effectively removed by the PATRIOT Act.

Plans to reorganise security intelligence structures in the US are a manifestation of the presidential need to be seen as being in control. The creation of the Department of Homeland Security (DHS) was apparently inspired by two main arguments: firstly, that the 'failure' of 9/11 was largely a failure to coordinate intelligence and security and, secondly, that a grand political gesture was required to convince the US public that 'something is being done' to improve security. The strategy of combining previously disparate security organisations in the apparent belief that improved hierarchical coordination will improve matters might well be criticised (for example, hierarchical forms of organisation are infamously poor at effectively developing and disseminating accurate information), but the main opposition to the plan in Congress was less about its wisdom *per se* than it was directed towards the accompanying presidential assertions of power. For example, the executive wanted to exempt the DHS both from rules governing access to information with respect to 'critical infrastructure' information;[2] from whistleblower protection (Mitchell and Hulse, 2002); as well as providing employees with fewer employment rights than elsewhere in the federal government (Allen and Mintz, 2002).

The original White House proposal for the DHS did not give much prominence to intelligence coordination. Finally the Act established a division for 'Information Analysis and Infrastructure Protection'. Its analyses and warnings would be developed from a combination of products passed on by the CIA, FBI and TTIC, and information gathered by, for example, border guards and secret service personnel who have been brought into the department (Pincus, 2002; Allen and Mintz, 2002). It remains to be seen whether the DHS will succeed in its aim of coordinating domestic security programmes within the notoriously fragmented US 'community', but the early signs are not promising. Members of Congress have criticised its lack of resources, including a shortage of computers with adequate

2. Editorial: 'Security. Not Secrecy', *Washington Post*, July 17, 2002.

security to receive 'top secret' data from the FBI and CIA (Mintz, 2003), and the possibility remains that it will become primarily a disseminator of NCTC assessments to state and local governments (Jordan, 2005).

The FBI itself has not escaped from the reorganisation efforts; as well as increasing the proportion of agents working on counterterrorism, CIA personnel were deployed to advise the Bureau on establishing its Office of Intelligence (Mueller, 2002). However, doubts remain about whether the Bureau can transform itself from a law enforcement agency into domestic security intelligence agency. There has been debate in Washington as to whether the US should separate the two functions as in the UK, and as Canada did in 1984 when the CSIS was established by separating out the RCMP Security Service (for instance, Joint Inquiry, 2002, pp. 349–53). The Kean-Hamilton inquiry into 9/11 considered this and recommended against it (2004, 13.5). Instead, the FBI is to create a National Security Service by merging its counterintelligence, counterterrorism and intelligence divisions with the head reporting to both the FBI Director and the new Director of National Intelligence (DNI) (Eggen & Pincus, 2005).

The CIA Director has never been able, in his dual role as Director for Central Intelligence (DCI), to coordinate the 'Intelligence Community' mainly because the Department of Defense controls the lion's share of the intelligence budget, about 80 percent, and is institutionally bound to see the main function of intelligence as support for the military. This flaw was exposed again by the Kean-Hamilton Commission and, following their recommendation (2004, 13.2) the Intelligence Reform and Terrorist Prevention Act 2004 established a new Director of National Intelligence (DNI) with greater formal authority over the 15 intelligence agencies. Initial signs are that, while the DNI's appointment reflects a loss of prestige and autonomy for the CIA, the Pentagon has retained its essential autonomy and the problem of coordinating the fragmented US system will remain (Ignatius, 2005; Pincus, 2005).

If executives are to deploy their new powers and organisations effectively, then they depend on intelligence. Some highly significant shifts have been made in an attempt to increase both the quantity and the quality of intelligence developed with respect to 'terrorism'; some changes are reflected in the law and some in executive assertions that earlier laws do not apply. The clearest example of the latter is detention without trial, both of two US citizens and 1,200 non-citizens (Seelye, 2002). The clear purpose of this is to gather information; bringing people to 'trial' before military commissions has been only a subsidiary consideration. The desire to gather information has led not only to the US agencies cooperating abroad with agencies long-associated with human rights abuses but also transferring individuals arrested in one country to others such as Egypt, Jordan and Morocco where torture is an established part of interrogation procedures. Transnational information exchange is one thing, brokering the use of torture is surely another. Further controversy developed in 2004 regarding the torture and abuse of detainees in Afghanistan, Guantanamo and Iraq (Greenberg & Dratel, 2005). In Canada the case of Maher Arar, who was 'rendered' to Syria in 2002, is being investigated by a judicial commission (http://www.ararcommission.ca). The UK Security Service told a hearing of the UK Special Immigration Appeals

Commission (SIAC – which hears challenges to Minister's decisions on detention and deportation on security grounds) that information obtained *via* torture will be assessed along with everything else (Gillan, 2003; Gumbel, 2003), despite torture being a clear breach of Article 3 of the European Convention of Human Rights (ECHR).

Regarding technical intelligence (TECHINT), executives in both the US and Europe are seeking improved access to electronic data. For example, the European Union has amended its 1997 Directive on Privacy so that the obligation of communications service providers to erase traffic data is superceded by an obligation to retain that data for 12–24 months (Peers, 2003). Documents obtained through the FOIA in the US show that under the PATRIOT Act there is increased use of 'national security' letters under which banks, ISPs, telephone and credit companies, etc., can be compelled to hand over customers' records. Prior to the Act the government had to show 'probable cause' but now they do not and companies are prohibited from telling anyone of the disclosure.[3] In the UK, the Regulation of Investigatory Powers Act (RIPA) 2000 already included similar powers. The EU and USA are also discussing an information exchange agreement between Europol and US agencies that does not include the normal EU data protection provisions (Peers, 2003).

The urge for more information is hardly surprising but does reflect some misunderstanding of just what kind of failure 9/11 represented. Arguably, too much congressional and media discussion since 9/11 has centred on the search for pieces of information that would, it is assumed, have enabled the 9/11 attacks to be predicted and then prevented. If not the search for the 'smoking gun' then perhaps the search for the 'smouldering datum'! Given what is known about the *modus operandi* of those carrying out the attacks, it is extremely unlikely that such information could realistically have been obtained. Certainly there were failures in gathering prior to 9/11, for example, the failure of FBI and CIA (Baer, 2002) to develop human sources at home and abroad. But the US intelligence community was already awash with data and it is far from clear that increasing the flow further will enhance the ability to prevent further 'failures'.

The real failure of US intelligence was the failure of processing and analysis (for example Whitaker, 2002). Analysts have always been the poor relations of gatherers within intelligence communities – they enjoy neither the reputation for 'derring-do' associated with human intelligence (HUMINT) nor the capacity to generate large profits for equipment suppliers associated with TECHINT. The key conclusions of the Congressional Joint Inquiry are highly pertinent; the information received that terrorists were contemplating the use of aircraft as weapons:

> did not stimulate any specific intelligence community assessment of … this form of threat (…) the community too often failed to focus on (available) information and consider and appreciate its collective significance … (Joint Inquiry, 2002, p. xi).

3. See: http://www.aclu.org/SafeandFree, March 24, 2003.

Given the almost complete absence of strategic analysts working on al-Qaeda, the general inexperience and lack of analytical training, the poor collaboration between analysts in different agencies, and the lack of language skills (Joint Inquiry, 2002, pp. 336–45), it is clear that the US intelligence community simply was incapable of preparing such assessments.

## Oversight and Review of 9/11

### *The Contest for Information*

Oversight is an extremely difficult task to perform in the security intelligence area if for no other reason than the all-pervading secrecy. The normal dependence of overseers for information on the agencies themselves may result in undermining of the whole process. Therefore, there have been significant struggles over 'information control' between executive (and agencies) and oversight bodies. This is not a new issue – the notion of 'executive privilege' in the US and the UK Official Secrets Acts has always been premised on the belief that executives should determine what security information, if any, is passed to assemblies. For example, the UK Intelligence Services Act 1994 states explicitly that the 'gatekeeper' for information made available to the Intelligence and Security Committee is the Minister (cf. Gill, 1996).

However, since 9/11, counterterrorism has been viewed more emphatically as a 'war' with consequently greater emphasis given by executives to 'secrecy' (both as counterintelligence and as an essential prerequisite for 'surprising' enemies). There are several areas in which the US executive has sought to reduce the flow of information: in a memo to federal agencies, Attorney General Ashcroft encouraged resistance to freedom of information requests – not in relation to security but more broadly in relation to 'institutional, commercial and personal privacy interests' (Borger, 2002; Rosen, 2002). Also, the Congressional Judiciary Committees criticised the Justice Department for seeking to deny information regarding its counterterrorism policies under the PATRIOT Act (Eggen, 2002).

The Joint Inquiry into 9/11 established by the two intelligence committees has also been critical of attempts by the executive to deny them access to information; for example, the refusal by the FBI to make available for testimony an informer and his handler (Risen, 2002; Joint Inquiry, 2002, p. 19), and that of the Director of Central Intelligence to declassify references to the intelligence community providing information to the White House (Hill, 2002). For those more familiar with parliamentary regimes, this denial is probably less surprising. For example, in the Canadian Security Intelligence Service Act 1984, cabinet documents are explicitly excluded from the general rule that SIRC has access to all information (CSIS Act, s. 39). In the US, the executive has also complained about the leaking of information from House and Senate Intelligence Committees regarding the National Security Agency (NSA) interception of two 'warning' messages on 10 September 2001 that were not translated until 12 September. In the face of these complaints, the committee chairs requested an FBI investigation into

the leaks (Allen and Eilperin, 2002). Thus the answer to the question 'who guards the guards?' is … 'the guards'!

*Internal Oversight*

The pressure on overseers to 'look the other way' is likely to increase following failures such as 9/11 and nowhere will this be greater than at levels one and two (see Figure 12.1) where there will be enormous political pressure on the ministries and agencies to deliver. Little has emerged on how these 'internal' oversight bodies have been performing since 9/11, but one example is the US Inspector-General in the Justice Department who reported 'significant problems' in the way hundreds of immigrants were treated as part of the 9/11 investigation with many being jailed for months without charge or access to lawyers (Lichtblau, 2003b). Another Inspector-General Report later confirmed the image of a dysfunctional intelligence community by showing the confusion among FBI personnel allocated to work at the CIA's Counterterrorism Center from 1996 onwards as to the exact nature of their role (Whitelaw, 2005).

*Legislative and Other Committees*

There have been a number of US congressional investigations of the 9/11 failure. For example, a report of the Subcommittee on Terrorism of the House Intelligence Committee noted in particular the lack of HUMINT within the CIA and poor dissemination to other agencies; that FBI counterterrorism was hindered by decentralisation and the culture of 'crime fighting'; and that the NSA needed to be more proactive in gathering intelligence (STHS, 2002). The major congressional effort in the year following 9/11, however, was a joint inquiry by the two intelligence committees. This identified seven areas of investigation, including: evolution of the terrorist threat to the US and the government's response; what the intelligence community knew prior to 9/11; what the intelligence community has learned since 9/11 about perpetrators and clues to explaining the failure; what has emerged about systemic problems impeding the community; how the intelligence community interacts with each other and the rest of the government in countering terrorism. The main conclusion on the specifics of 9/11 was that:

> While the intelligence community had amassed a great deal of valuable intelligence regarding Osama Bin Ladin and his terrorist activities, none of it identified the time, place, and specific nature of the attacks that were planned for September 11, 2001. Nonetheless, the community did have information that was clearly relevant to the September 11 attacks, particularly when considered for its collective significance (Joint Inquiry, 2002, p. xi).

More broadly with respect to US counterterrorism efforts, the Joint Inquiry concluded that the intelligence community was 'neither well organised nor equipped', serious gaps existed in the collection coverage provided by the agencies, the foreign intelligence agencies paid inadequate attention to the

potential for attacks within the US, and there was no effective domestic intelligence capability (Joint Inquiry, 2002, p. xv).

The concern of senior members of the Inquiry at what they described as inadequate cooperation with the executive branch led them to endorse the idea that a separate commission of inquiry into 9/11 should be established. This idea was supported by the families of victims of 9/11 but the White House initially opposed the idea, saying it would distract the agencies from their primary task. However, after further wrangling between the White House and Congress, an agreement was reached just before Congress adjourned in 2002, and a Commission of ten members was established. Their report was published in July 2004 and identified general failures of imagination, policy, capabilities and management throughout US government. More specifically it dealt with shortcomings in diplomacy, border security, military options and intelligence and made many recommendations regarding future strategies and organisation (Kean & Hamilton, 2004).

In Canada the main burden of oversight at the third level is the responsibility of the Security Intelligence Review Committee (SIRC). Members are appointed by the Prime Minister and serve part-time. SIRC has a full-time staff of 16 and two main functions: to review the activities of CSIS, and to investigate complaints about the service. The Committee may also hold hearings on challenges to CSIS security assessments. Overall, SIRC regards its role as reviewing whether CSIS 'has acted appropriately and within the law' (SIRC, 2002, p. 3). Building on previous reviews of CSIS counterterrorism work, SIRC established the following objectives for its study: 'the reach and focus' of CSIS investigation of Sunni Islamic extremist activities; the 'nature and quantity of assessments, analyses and other advice disseminated to government and law enforcement; and the 'character and quantity of information exchanges' with allied services (SIRC, 2002, p. 5). SIRC made no claim that its review was comprehensive, saying that it concentrated on how the Service ran its investigation, its analytical outcomes and the advice disseminated to government. Its conclusion was very similar to that of the US Joint Inquiry Staff Report quoted above:

> Although none of the intelligence products or threat warnings we reviewed pointed directly to the events of September 11, the service clearly was aware of the potential for Al Qaeda inspired terrorist attacks of some kind and communicated this information to the appropriate bodies in government. In the Committee's view, however, none of the advice or communications the Committee reviewed warned of a threat sufficiently specific in time or place to have alerted government authorities to the events of September 11 (SIRC, 2002, p. 7).

In comparison with the extensive external inquiries in the US and even the more modest SIRC inquiry, the UK inquiry into 9/11 was minimal. The ISC Annual Report (2002a) identified some resource pressures in the Security Service, Secret Intelligence Service and Defence Intelligence Staff (para. 61); referred to a Joint Intelligence Committee July 2001 assessment that al-Qaeda attacks were in the final planning stages but that timings, targets and methods were unknown (para. 65); noted the redeployment of staff post-9/11 (paras. 67–69); noted the increased

Security Service resources in collection and dissemination (para. 72); but, significantly, said nothing about analytical deficiencies. Finally, it noted the lack of linguists (para. 77). The ISC carried out an examination of the intelligence, assessments and travel advice regarding Indonesia after 200 people (mainly Australians but including 24 British) were killed in a nightclub bombing in Bali in October 2002. Again, their conclusion was that 'on the available intelligence there was no action that the UK or its allies could have taken to prevent the attacks' (ISC, 2002b, p. 5). However, the Committee did criticise as a 'serious misjudgement' the failure of the Security Service to increase the level of threat to British interests from three (significant) to two (high) on the six-point scale so that the Foreign Office's travel advice could have been amended before October (ISC 2002b, pp. 5–6). It is understood that the Security Service did not accept this conclusion.

Comparing these reports, it is not surprising that they were all concerned overwhelmingly with the issue of efficacy – was there anything that the agencies could have done to prevent the attacks? The only acknowledgements of propriety issues are a brief reference by Congress on the need for intelligence to be conducted within the rule of law (Joint Inquiry, 2002, pp. 353–354), and the SIRC comment that their review did not examine the compliance with law and policy of CSIS warrants and handling of human sources (SIRC, 2002, p. 5). It is also important to note the significant methodological differences between these reviews, largely, though not entirely determined by the availability of staff. The US Joint Inquiry team had 24 researchers divided into five investigative teams that interviewed officials, reviewed documents and submitted questionnaires not only at the FBI, CIA and NSA, but also other departments (Hill, 2002). We might assume that at most about ten of SIRC's staff would have been involved in its 9/11 inquiry and they made no claim to have examined 'all the raw intelligence' available to CSIS (SIRC, 2002, p. 5), but these staff would also have carried out interviews and reviewed documents. The UK effort, by comparison, was hampered from the start by the fact that half of the nine-person committee (including the Chair) was newly appointed after the 2001 election. The members themselves 'took evidence' over the year from 37 witnesses (Ministers, Heads of Services and other officials) and made 'visits' to the agencies. But what might properly be described as 'investigative' work fell to the single investigator who was tasked to carry out five investigations during the year, none of which appear to have concerned 9/11 (ISC, 2002a, pp. 5, 29–31). The conclusions reached by the ISC appear to have been based entirely on briefings from agency heads; at least, there is nothing in the report to lead one to suppose otherwise.

*Courts and Judges*

It is in the US where security intelligence issues are most likely to end up in court, though even here, special arrangements have been made to hear some cases, for example, Foreign Intelligence Surveillance Act (FISA) courts. But the Bill of Rights remains a fertile field within which lawyers have sought to test the constitutionality of some of the executive and legislative measures taken since

9/11. For example, federal judges in various parts of the country have ordered an end to secret deportation hearings, have tried to limit the executive's use of the material witness law to sustain unlimited detention, and have ordered the executive to publish the names of the 1,200 people detained after 9/11.[4] A federal judge in Los Angeles ruled as unconstitutional a 1996 law making it a crime to provide 'material support' to any foreign organisation deemed by the State Department as 'terrorist' on the grounds that groups have no chance to defend themselves (Winter, 2002), but prosecutors continue to use the law pending appeals and the Supreme Court has so far avoided hearing fast-tracked challenges to the constitutionality of the new anti-terrorist laws.

In the UK, one of the most controversial elements of the Anti-Terrorism, Crime and Security Act was that it empowered the government to detain without trial non-citizens who the government could not deport because of fears for their safety in their home country. SIAC ruled this to be discriminatory and therefore contrary to the Human Rights Act 1998 because it applied only to non-British citizens. The House of Lords upheld this decision in December 2004 prompting the government to pass the Prevention of Terrorism Act 2005 that replaced indefinite detention with the possibility of 'control orders' including electronic 'tagging' and house arrest for terrorist suspects.

*Media and Groups*

Finally, what examples have there been of 'oversight' taking place at level four? Firstly, a number of the cases reported above have been challenges supported by civil liberty groups such as the American Civil Liberties Union, which has filed 24 relevant lawsuits since 9/11 (Scheeres, 2002), and Liberty in the UK. Secondly, there have been efforts at more wide-ranging critiques of executive initiatives; for example, the Electronic Privacy Information Center (EPIC) and Privacy International produced a joint report regarding the impact of current and proposed laws in 50 countries since 9/11. It identifies four main trends: swift erosion of pro-privacy laws (as in the EU example above); greater data sharing between corporations, police and security agencies; greater eavesdropping (see above); and sharply increased interest in people-tracking technologies (McCullagh, 2002). The media in general remains a significant, if inconsistent, contributor to oversight. Certainly, the heightened public concern with security in the wake of 9/11 has increased media attention on intelligence matters and has played an important role in alerting the public to concerns among intelligence professionals at the politicisation of their product. However, bitter battles over information control have resulted and their long-term impact on the relationship among governments, their intelligence agencies and media could be problematic. In the case of Iraq, for example, rows involving the BBC (see further below) and, in the US, CBS and Newsweek have indicated that, in matters of national security, it may be easier to hold media accountable for their errors than governments!

4. Editorial 'Secrecy vs. the Republic,' *Los Angeles Times*, August 6, 2002.

**Intelligence, Politics and Oversight: The Lessons from Iraq**

Intelligence goes to the very heart of the functions of the state and the exercise of power. Therefore, in all of the discussions about new laws and rules for the conduct and oversight of intelligence, it must be remembered that intelligence and oversight are essentially political activities. This has been dramatically confirmed by the controversies around the role of intelligence in the lead up to the invasion of Iraq in 2003. In the space available it is only possible to discuss briefly two main points: the need for critical examination of both the relationship between knowledge (intelligence) and power (policy), and the performance of overseers lest they become too close to power.

On the first, from the extensive inquiries carried out in the UK and US, it is now clear that the decision to invade was made independently of any intelligence that might have supported that policy. Much of the furore since the emergence of the fact that Iraq possessed no weapons of mass destruction (WMDs – the only basis on which the invasion could have been rationalised under international law) has centred on the 'intelligence failure' this indicated. Certainly there was an intelligence failure in that the combined efforts of US and UK human and technical intelligence gathering failed to discover that most WMDs had been destroyed by the Iraqis or UN inspectors after 1993 but, arguably, there was an even greater political failure. This took two main forms: first, the decision to invade was taken largely independently of the intelligence; and, second, such intelligence as there was regarding Iraqi WMDs was used highly selectively and exaggerated during the lead up to the invasion. While the evidence of 'intelligence failure' has been picked over in great detail in the US by the Senate Select Committee on Intelligence (SSCI, 2004) and the Silberman-Robb (2005) inquiries and, in the UK, to a greater or lesser extent by the Foreign Affairs Committee (FAC, 2003), the ISC (2003b), and the Hutton (2004) and Butler (2004) inquiries, the question of political failure has been left relatively undisturbed.

In the UK, the controversy was ignited in late May 2003 by a BBC broadcast to the effect that the government had inserted information into its September 2002 dossier (HMG, 2002) despite knowing that the information was false. In the context of the failure to find the alleged WMDs, the Commons Foreign Affairs Committee (FAC) investigated, although their efforts were hampered by their general lack of access to relevant papers and people. The FAC report concluded that the government's decision regarding the seriousness of the threat posed by Iraq was justified on the basis of the information available at the time but noted that the UK had been heavily reliant on US intelligence. Furthermore, it was critical in a number of ways of the politicisation of intelligence – that claims were asserted with more certainty than was justified, that political advisers had chaired meetings on intelligence matters, and that Blair misrepresented as 'further intelligence' a dossier that included previously published research plagiarised from the internet (FAC, 2003).

The government's response to the furore was to ask the ISC to investigate – the advantage to Blair being that this Committee would conduct its proceedings in secret and send its report to him before it would be published minus any 'national

security' exclusions. The ISC enjoyed more access to people and papers than the FAC. In July, once he had been identified, the government ensured that the identity of the source for the original BBC broadcast was publicised – he was Dr David Kelly, an international expert on biological warfare who had been a central member of UN inspection teams. He was immediately required to give evidence to both the FAC and ISC inquiries but was found dead the following day. This added fuel to the controversy and Blair appointed a House of Lords judge, Lord Hutton, former Chief Justice of Northern Ireland, to conduct an investigation into the circumstances surrounding Kelly's death. While Hutton was still investigating, the ISC published its report. Based on the intelligence it had seen:

> there was convincing intelligence that Iraq had active chemical, biological and nuclear *programmes* and the capability to produce chemical and biological weapons (ISC, 2003b, para. 66, emphasis added).

On the controversial September 2002 dossier, the ISC concluded:

> The dossier was for public consumption and not for experienced readers of intelligence material.... The fact that it was assessed to refer to battlefield chemical and biological munitions and their movement on the battlefield, not to any other form of chemical or biological attack, should have been highlighted in the dossier. *This was unhelpful to an understanding of the issue*' (2003b, para. 86, emphasis added).

In retrospect, Hutton's inquiry was significant mainly for the fact that he immediately published almost all the written evidence he received on the Inquiry website and heard open testimony because his findings – that the BBC was entirely to blame for the fiasco while the government had acted properly throughout – were greeted with widespread scepticism and disdain. (Gill, 2005; see Glees & Davies, 2004 for a different view of Hutton.) Hutton followed his narrow terms of reference strictly and therefore did not address the wider issue of the accuracy of the government's Iraq dossier. The government's hope that Hutton would put an end to the controversy was immediately derailed by this and the simultaneous testimony of David Kay – the head of the Iraq Survey Group – informing the US Congress that the failure to find WMDs indicated that 'we were all wrong' (Stevenson & Shanker, 2004). So the Fourth inquiry was set up, this one headed by Lord Butler and including two members of the ISC among its team. Unlike Hutton, Butler conducted his inquiry in secret and, when he reported in July 2004, reached broadly similar conclusions as the ISC to the effect that it was a 'serious weakness' that the September dossier did not include the caveats on the limits of the intelligence (Butler, 2004, para 465). Butler did go further and observed that:

> The Prime Minister's description, in his statement to the House of Commons on the day of publication of the dossier, of the picture painted by the intelligence services in the dossier as '*extensive, detailed and authoritative*' may have reinforced this impression (para. 464, emphasis in original).

The word 'may' here is crucial – a reading of the Joint Intelligence Committee (JIC) assessments of Iraqi WMDs in 2002 when compared with the language in the dossier and the Prime Minister's speech to the House of Commons make it abundantly clear that the Prime Minister did mislead parliament. (Gill, forthcoming, examines this in detail. See also Danchev, 2004). If so, why did Butler not say so? The answer lies in the reticence of the recently-retired Whitehall civil servant. At a subsequent appearance before the Commons' Public Administration select committee Butler indicated the unwillingness to reach a 'political' rather than 'legal' conclusion:

> On the political issues, we wanted to give people the information but we felt that really the proper place where governments should survive or fall is with parliament and the electorate…It would have been a heavy responsibility and one where it would have been improper for us to say that we think the government should resign on this issue (Sparrow, 2004).

The issue of whether or not there was political pressure on analysts to adjust their findings to policymakers' preferences was addressed more carefully by the SSCI but the only critical evidence regarding the pressure on analysts in their report is in the 'additional views' of some Committee members (SSCI, 2004, 455–457). The Democratic minority agreed in February 2004 to postpone reporting on the politically more contentious issue of the government's use of intelligence until after the presidential election in November (SSCI, 2004, 2). However, after the presidential election, and in an act of political forbearance similar to Butler's, it emerged that the second report had been quietly dropped. Silberman-Robb (2005) repeated the by now well-known catalogue of intelligence failures but felt prevented by their terms of reference from examining how the government had (mis)used intelligence.

Final proof that the Iraq invasion was a case of policy preceding intelligence rather than the other way around came in the UK with the leak of several key documents from 2002 to a journalist. The Iraq controversies seem to have ruptured the normally secure intelligence community in Whitehall since the memos indicate clearly that Blair had agreed in April 2002 that the UK would support military action to bring about regime change in Iraq. Since this was illegal, some pretext had to be found. This was to take various forms including persuading the UN Security Council to give Saddam Hussein an ultimatum to allow in weapons inspectors and increasing the bombing of Iraq through the Summer and Autumn of 2002 in the hope of provoking retaliation (Smith, 2005a; Smith 2005b; Bamford, 2005 and Hiro, 2005 provide fuller analyses of the lead up to war). Thus the role of intelligence was to provide support to the invasion policy as the lamppost provides support, not illumination, to the drunk. Intelligence with respect to the *lack* of evidence of WMDs or Iraqi links with al-Qaeda or that an invasion might actually worsen the problem of terrorism was simply ignored.

## Conclusion

What are the lessons for the future of the control and oversight of intelligence of this necessarily brief review of developments since 9/11? Clearly, these are still working through intelligence and governmental systems across the world and will do so for the foreseeable future. It is not possible to predict the direction of these changes given the uncertainties surrounding the course and consequences of the 'war on terror'. But if much has changed in the security intelligence world in the past three years, it is still important to maintain a grasp on some hard-learned lessons so that the democratic gains of the 1990s are not squandered in a security panic in the 2000s.

We should not accept the 'balance' metaphor – rights relating to privacy, speech and freedom from torture cannot simply be 'weighed' against security factors. Limitations on rights can only be justified in terms of proportionality to the nature and size of the security threat (Leigh & Lustgarten, 1994). Reductions in rights and freedoms do not make for greater security; they make for less democratic societies in which the possibilities of abuse and harm by the state or vengeful populations are increased. If those waging the 'war on terror' are prepared to use torture, unlimited detention without trial and unprecedented invasions of privacy, then the renewed need for vigorous control, oversight and review of state security intelligence activities is clear.

Since oversight bodies are often small, they must cooperate with each other, including sharing information whenever possible subject to minimal necessary secrecy requirements. The trap to be avoided is that oversight itself becomes compartmentalised as it is in the UK, where the government still denies the parliamentary committee access to the confidential annexes of reports made by the judicial commissioners regarding interception warrants. Although the term intelligence 'community' often attracts hollow laughter because of the interagency conflicts and 'turf wars' that take place, we must acknowledge that ever-increasing information sharing is occurring both within and between public and private intelligence sectors. This is clearly necessary in the interest of efficacy but also heightens the risk of potential abuse, for example, by the subcontracting of operations to agencies less imbued with a culture of human rights. Oversight bodies, both within and among different countries, must seek to assist each other – what is needed is an *oversight community*. This is now beginning to emerge. For example, there are regular interchanges between oversight committees (including those in the 'newer' democracies), and there are biennial meetings of the International Intelligence Review Agencies' Conference (ISC, 2003a, 6). So far these conferences have been private affairs; it would help if at least some part of their proceedings were held in public.

Third, overseers must be continuously vigilant lest they be denied relevant material or be otherwise misled. On more than one occasion members of the Silberman-Robb Commission had to remind President Bush of their threat to resign if they were denied cooperation by the agencies (Waterman, 2005). In the post-9/11 environment it is natural that oversight bodies have been primarily concerned with their agencies' effectiveness and, as we have argued, this is entirely in line

with overall democratic control of intelligence. But it is important that they beware of incorporation by agencies into management, rather than oversight, tasks. All oversight bodies owe important duties to uphold human rights and liberties and thus their engagement with the agencies must always retain a critical and sceptical approach in order to retain hard-won democratic gains. In turn, there is a duty on citizens, NGOs and media to check that formal oversight bodies do maintain this approach.

# PART V

# Data Protection

*This page intentionally left blank*

Chapter 13

# Public Oversight and National Security: Comparative Approaches to Freedom of Information

*David Banisar*

**Introduction**

Access to government records and information is an essential requirement for developing and maintaining a civil and democratic society. It provides an important guard against abuses, mismanagement and corruption. It can also be beneficial to governments themselves – openness and transparency in the decision making process can assist in developing citizen trust in government actions. This is especially true for access to information about intelligence services and other national security bodies where the bodies in many countries have a history of secrecy and abuse.

There is a global trend towards government transparency. Governments around the world are increasingly making more information about their activities available. Over 60 countries around the world have now adopted comprehensive Freedom of Information (FOI) Acts to facilitate access to records held by government bodies and over thirty more have pending efforts.[1]

Most countries also have laws relating to the classification and protection of national security information. These laws, some of which have been in place for many decades, often conflict with the FOI laws. Information about government bodies is frequently withheld for national security reasons in an overly broad manner that has little to do with protecting the state. This article will review the global trends towards FOI laws and its impact on national security.

1. Detailed information about FOI laws around the world, and in particular those quoted in this article, can be found in David Banisar, 2006.

**History of FOI Laws**

Freedom of information has been recognised for nearly 250 years. Sweden adopted its Freedom of the Press Act in 1766 (Lamble 2002). Meanwhile, other European countries also promoted transparency. The Dutch 1795 Declaration of Rights of Man stated, 'That every one has the right to concur in requiring, from each functionary of public administration, an account and justification on his conduct'. The 1789 French Declaration of the Rights of Man and of the Citizen called for the right of citizens to review expenditures of the government and the right of society to demand an accounting of the administration of a public official.[2] Over the years, access became more common to debates in parliaments and the opening of most courts but not necessarily for administrative bodies. Most intelligence bodies were completely exempt to the point of not even being officially recognised as existing.

At its first session in 1946, the General Assembly of the United Nations recognised that 'Freedom of information is a fundamental human right and is the touchstone of all the freedoms to which the United Nations is consecrated'.[3] This was incorporated into Article 19 of the 1948 UN Declaration of Human Rights which states:

> Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers.

In the following years, countries slowly began to enact comprehensive laws for access to government-held documents and information: Finland enacted its law in 1951;[4] the United States enacted its Freedom of Information Act in 1966;[5] France and the Netherlands in 1978;[6] Australia and New Zealand in 1982;[7] and Canada in

2. The Declaration of the Rights of Man and the Citizen, 1789, available at: http://www.diplomatie.gouv.fr/france/14juillet/gb/decldroits.html.
3. Resolution 59(1), 14 December 1946.
4. Act on Publicity of Official Documents, Finland, Act 83/9/2/1951.
5. Freedom of Information Act, 5 USC 552, 1966, available at: http://www.epic.org/open_gov/foia/us_foia_act.html.
6. Law No. 78-753 of 17 July 1978 on the freedom of access to administrative documents; Law No. 79-587 of July relating to the motivation of administrative acts and the improvement of relations between the administration and the public. Amended by Law No. 2000-321 of 12 April 2000 relating to civil rights in relation with the administration (J.O. of 13 April 2000), available at: http://www.legifrance.gouv.fr/texteconsolide/PPEAV.htm; English version available at: http://www.cada.fr/uk/center2.htm; The Netherlands, Act on Public Access to Information of 9 November 1978. Replaced by Act of 31 October 1991, containing regulations governing public access to government information, available at: http://www.minbzk.nl/contents/pages/00012478/public_access_government_info_10-91.pdf.
7. Australia - Freedom of Information Act 1982, available at: http://www.austlii.edu.au/au/legis/cth/consol_act/foia1982222/; New Zealand Official Information Act 1982, available at: http://www.ombudsmen.govt.nz/official.htm.

1983.[8] The last ten years has been the most active period of countries adopting freedom of information laws with over half of the countries adopting their laws during this time.

In 2004, nearly all of the countries in the northern hemisphere have adopted comprehensive FOI acts. In Western Europe, only Luxembourg, Malta, and Cyprus lack legislation and most Central and Eastern European countries have recently adopted laws as part of their transitions to democracy.[9] The rest of the world is also moving in the same direction. The trend has progressed globally and laws are found in all regions and continents. In Asia, India, Pakistan, Japan, Thailand, and South Korea have adopted laws and a number of other countries are currently considering bills. Even in China, a few localities have adopted transparency laws. In South and Central America, half a dozen countries have adopted laws and almost every other country is currently considering them. In Africa, Angola, South Africa and Uganda have adopted FOI laws and many others on the continent including Nigeria, The Ghana and Kenya are currently considering similar acts.

There are also sub-national FOI laws at the provincial, state and municipal levels in many countries including Argentina, Australia, Canada, Germany, India, Japan, Mexico, Switzerland, and the United States. In Japan, nearly 3,000 local municipalities have adopted FOI ordinances.

Finally, many other laws such as administrative procedure acts and environmental, consumer and data protection laws often include provisions giving individuals the right to access some information to protect their interests. Other laws require publication of information for public interest reasons and include laws on archives, statistics, elections and political parties as well as anti-corruption.

*Factors for Adoption*

There have been a variety of internal and external pressures on governments to adopt FOI laws. International organisations and civil society groups have played a key role in the promotion and adoption of laws in many countries. This has included campaigning by press and environmental groups. Governments are providing more access to information as part of their 'e-government' efforts to make services more efficient and accessible.

*International pressure* International bodies promoting good governance and anti-corruption have played a key role in pressuring countries into adopting transparency measures. The World Bank, the International Monetary Fund and others have pressed countries to adopt laws to reduce corruption and to make financial systems more accountable.[10] The UN has also recognised the importance

8. Access to Information Act, Canada, C. A-1, available at: http://canada.justice.gc.ca/STABLE/EN/Laws/Chap/A/A-1.html.
9. See Banisar, 2004.
10. See IMF, *Manual on Fiscal Transparency*, available at: http://www.imf.org/external/np/fad/trans/index.htm.

of access.[11] The UN Convention on Corruption, approved in October 2003, calls on governments to protect the right of citizens to access information to fight corruption.[12] The Rio Principles released by the 1992 UN Earth Summit call for increased access to information on the environment held by public authorities to enhance citizens' participation in decision-making about environmental matters.[13] The 1997 UN/ECE Convention on Access to Information, Public Participation in Decision-Making and Access to Justice in Environmental Matters (the Aarhus Convention) has been signed by forty countries.[14]

*Regional bodies* The role of regional bodies has also been important. The Council of Europe has provided assistance to numerous countries in Central and Eastern Europe, the Balkans and Caucuses on developing and implementing laws. It issued detailed guidelines on access laws in 2002 and recently began efforts to develop the first international treaty on access to information.[15] The Commonwealth first issued a resolution in 1980 encouraging its members to adopt access laws and has followed it with principles in 1999 and a model bill in 2003.[16] The European Union has adopted two directives requiring national governments to adopt laws guaranteeing access to environmental information as well as other directives incorporating provisions on rights of access relating to the environment, human rights and procurement.[17] The Organisation of American States (OAS) has helped develop bills in Guatemala and other countries in the region. Other regional conventions such as the 1992 Convention for the Protection of the Marine Environment of the North-East Atlantic (OSPAR) also provide a right of access.

*Constitutional rights* The transition to democracy for most countries has led to the recognition and incorporation of human rights in constitutions. Almost all newly

11. The UN Commission for Human Rights has refered to the Johannesburg Principles on National Security, Freedom of Expression and Access to Information, U.N. Doc. E/CN.4/1996/39, 1996.
Available at: http://www1.umn.edu/humanrts/instree/johannesburg.html.
12. See Report of the Ad Hoc Committee for the Negotiation of a Convention against Corruption on the work of its first to seventh sessions, 7 October 2003, available at: http://www.unodc.org/unodc/en/crime_convention_corruption_reports.html.
13. Principle 10, Rio Declaration on the Environment and Development, available at: http://www.un.org/documents/ga/conf151/aconf15126-1annex1.htm.
14. UNECE, available at http://www.unece.org/env/pp/.
15. Council of Europe, Recommendation Rec(2002)2 of the Committee of Ministers to member states on access to official documents, 2002, available at: http://cm.coe.int/stat/E/Public/2002/adopted_texts/recommendations/2002r2.htm.
16. Commonwealth Secretariat, Freedom of Information Act, May 2003, available at: http://www.thecommonwealth.org/law/docs/Freedom%20of%20Information%20-%20revised%20on%207%20May%2003.doc.
17. Directive 2003/35/EC of the European Parliament and of the Council of 26 May 2003 providing for public participation in respect of the drawing up of certain plans and programmes relating to the environment; Directive 90/313/EEC of 7 June 1990 on the freedom of access to information on the environment.

developed or modified constitutions include a right to access information from government bodies. Over 40 countries now have constitutional provisions on access. They also often include provisions on a right to information on the environment and the right of individuals to access their personal files. Most countries which have a constitutional right have subsequently adopted laws on access. Courts in the Philippines, Chile and Uganda have ordered government bodies to provide information under the Constitutional provision, even in the absence of a FOI law. The Indian Supreme Court in 2002 ordered the Election Commission to make candidates for political office publish information about their criminal records, assets, liabilities and educational qualifications.[18] This led to the adoption of a comprehensive national act.

*Scandals* Crises caused by a lack of transparency have often led to the adoption of laws to prevent future problems. In long-established democracies such as Ireland, Japan and the United Kingdom, laws were finally adopted as a result of sustained campaigns by civil society and political scandals relating to health, the environment and corruption.

*Modernisation and the Information Society* The expansion of the Internet into everyday usage has increased demand for more information by the public, businesses and civil society groups. Inside governments, the need to modernise record systems and the move towards e-government has created an internal constituency that is promoting the dissemination of information as a goal in itself. In Slovenia, the Ministry for the Information Society was the leading voice for the successful adoption of the law.

## A Brief Comparison of Laws

Generally, FOI laws in most countries have a common design. The basic elements are: the right of an individual to be able to demand information from government bodies without having to show a legal interest; the duty of the body to respond and provide the information; exemptions to allow withholding certain categories of information because of the harm the release would cause; internal appeal mechanisms; and some form of external review. There is also often a requirement for government bodies to affirmatively publish some types of information about their activities.

The most basic feature of FOI laws is the ability to ask for materials held by government departments. This is variously defined as records, documents or information. Definitions of 'information' determine the scope of the legislation. In many laws, differences in definitions have led to gaps in access as computers have

18. Union of India *vs* Association For Democratic Reforms. Civil Appeal No 7178 of 2001, available at: http://www.privacyinternational.org/countries/india/india-v-adr-foia-502.pdf.

replaced paper filing systems. Newer laws broadly define the concept so that there is little difference between these two systems.

The right to request information is generally granted to citizens, permanent residents and corporations in the country without a need to show a legal interest such as an injury that needs the information to remedy the harm. The majority of laws can be used by anyone around the world to ask for information. The US Freedom of Information Act, in particular, has been used by newspapers and NGOs in countries where there is no such act to highlight the lack of information available in the country.

Access is generally limited to information which is already recorded. Many Western European laws provide and regulate access to 'official documents' only, which does not include drafts and other internal documents. Certain laws do require the creation of documents: the Irish Freedom of Information Act requires that departments provide a written explanation of decisions that affect their interests; the Danish Access to Public Administration Files Act requires authorities to record information of importance. In some jurisdictions, such as Austria and under the UK Code of Access to Information (soon to be replaced by a full FOI law), the duty is only to provide information or answer questions, not to provide the original documents.

*Coverage of Government Bodies*

Generally the acts apply to nearly all government bodies in the countries. In some countries, the parliament, courts, and the security and intelligence services are exempt from coverage.

There is a growing trend towards extending FOI laws in countries to include non-governmental bodies such as companies and NGOs that receive public money to do public projects or have some form of public decision-making authority. This includes privatised companies, government controlled corporations and government contractors. In South Africa, the law also allows individuals and government agencies to obtain information from private entities if it is necessary to enforce people's rights. Data protection acts and environmental laws in many countries provide for a right of access to certain categories of documents held by private bodies with no government connection.

As international governmental organisations play an increasingly important role, the right of access to information is evolving to address the new structures. Decisions that were once made on a local or national level where the citizen had access into the process are now being made outside the country in a more secretive setting because these organisations are based on a diplomatic system. A leading example of this is the European Union. The EU decisions are made by national government representatives in Brussels which are binding on all the member states. At the same time, the information access provisions are significantly weaker than most of the members laws.[19] Activists have also pressured the World Trade

19. Roberts, 2001.

Organisation (WTO), the World Bank and the IMF to release more information and they have become progressively more open but access is still limited.[20]

*Exemptions and Balancing*

All freedom of information laws recognise that there are circumstances under which information should not be released because it would harm public or private interests. Generally, these exemptions are included in the FOI law.

There are a number of common exemptions that are found in nearly all laws. These include the protection of national security and international relations, personal privacy, commercial confidentiality, law enforcement and public order, information received in confidence, and internal discussions. The Council of Europe suggested the following exemptions in 2002:

1. national security, defence and international relations;
2. public safety;
3. the prevention, investigation and prosecution of criminal activities;
4. privacy and other legitimate private interests;
5. commercial and other economic interests, be they private or public;
6. the equality of parties concerning court proceedings;
7. nature;
8. inspection, control and supervision by public authorities;
9. the economic, monetary and exchange rate policies of the state;
10. the confidentiality of deliberations within or between public authorities during the internal preparation of a matter.[21]

*Harm tests* Most FOI laws require that information be withheld on the basis of an exemption only after a government body has shown that harm will result from its disclosure. The test for harm generally varies depending on the type of information that is to be protected. National security, privacy, and international relations tend to get the highest level of protection.

*Public interest test* A number of countries including South Africa, Jamaica, Japan, Ireland, the United Kingdom, New Zealand and Bosnia require that a public interest test is applied for at least some exemptions. This provides for information to be released if the public benefit in knowing the information outweighs any harm that may be caused by its disclosure. This test can be applied both at the administrative level when a body is reviewing information for release and also at the appeals level when an independent commission or court is reviewing the body's decision.

In Japan, the head of the administrative organ is given the power for a discretionary release 'when it is deemed that there is a particular public interest

20. See IFTI Watch, available at http://www.freedominfo.org/ifti.htm.
21. Recommendation Rec.(2002)2 of the Committee of Ministers to member states on access to official documents, 21 February 2002.

necessity'. In South Africa, the Promotion of Access to Information Act (PAIA) requires that an information officer release the record if 'the disclosure of the record would reveal: evidence of a substantial contravention of, or failure to comply with, the law; or an imminent and serious public safety or environmental risk; and the public interest in the disclosure of the record clearly outweighs the harm contemplated in the provision in question'.[22] The Council of Europe Recommendations state that the documents should be released if 'there is an overriding public interest in disclosure'.[23]

*Other non-exempt information* Many FOI laws prohibit certain information from being withheld. This includes evidence of a crime or information on human rights abuses. The Mexican Federal Transparency and Access to Information Law provides that 'Information may not be classified when the investigation of grave violations of fundamental rights or crimes against humanity is at stake'. The Peruvian Law on Transparency and Access to Public Information prohibits the withholding of information relating to human rights abuses or violations of the Geneva Convention of 1949. The limits contained in the Georgian Freedom of Information Act include environmental hazards, descriptions of an agency's principles, structure, officials, elections, audits and election-related information. Most FOI laws provide that while internal discussions of policies can be exempted, the underlying factual information used to make the decisions cannot be.

In addition to exemptions based on substantive concerns, most FOI laws include provisions to reject FOI requests based on administrative concerns. These include information that is available by other means, will be published shortly, overbroad requests that would interfere with the operations of the body and 'vexatious' or repeated requests filed over and over again even though that have already been handled.

*Appeals and Oversight*

In all countries, the decision of the public body on the releasing and withholding of information is subject to review. In most countries, there is usually an internal review conducted by a higher-level authority and a final review by an independent external body. The courts are the final remedy in nearly all countries.

*Internal review* The first level of review in all but a few countries is an internal appeal. This typically involves designating a more senior official in the body or a superior department to review the withholding of information. Internal review can be an inexpensive and quick way of reviewing decisions and releasing more documents. However, the experience in some countries such as Australia is that

22. Promotion of Access to Information Act, South Africa, para. 46 'Mandatory disclosure in public interest'.
23. Recommendation Rec.(2002)2 of the Committee of Ministers to member states on access to official documents, 21 February 2002.

they most often uphold the denials and are not generally effective at enhancing access.

*External review* Nearly all countries have some form of external review which can be requested once the internal appeals have been completed to ensure that the decision by the government body was not flawed. Usually, under standard administrative procedural practice, internal appeals must be exhausted before external review can be requested. Some laws, such as those of the United States, provide also that a failure to respond is considered to be a denial and sufficient grounds to begin immediate litigation.

*Ombudsmen* The most common type of external body to review decisions is an ombudsman, typically a constitutional officer or a representative of the parliament. Ombudsmen generally do not have the authority to issue a binding decision on public bodies but in most countries their decisions are considered to be quite influential and typically are followed by government bodies. Generally, ombudsmen are limited to handling specific cases and often are not able to look more systematically at the overall system.

*Information Commissioners* Over twenty jurisdictions have created an independent body to review decisions. These information commissions can be part of the parliament, the Prime Minister's office (such as in Thailand) or an independent body.[24] The Commissioner's powers vary. In many jurisdictions, such as in Canada, they are similar to ombudsmen and are only given the power to issue opinions. In Mexico, Ireland and the United Kingdom, the Commissioner can make binding decisions. In Hungary, the Commissioner can only make recommendations in FOI cases but can order changes in the classification of state secrets.[25] In general the Information Commissioners can be tasked with many duties besides merely handling appeals. This includes general oversight on whether the system is working and also reviewing and proposing changes, training, and public awareness.

*Courts* Almost all countries allow the requester to appeal to the national courts. The courts generally are given the power to obtain copies of most records and make binding decisions. In some countries, the court can only review a point of law once a tribunal has made a decision. In others, requesters can appeal to the court instead of appealing to the ombudsman or information commission. Where the courts serve as the only external point of review, such as in the United States and Bulgaria, many users are effectively prevented from enforcing their rights

24. Information Commissioners depend on national bodies in Belgium, Canada, Estonia, France, Hungary, India, Ireland, Latvia, Mexico, Portugal, Serbia, Slovenia, Switzerland, Thailand, Turkey, United Kingdom and on the sub-national level in Australia, Canada, Mexico, the United Kingdom and Germany.
25. For the case of Hunagary, see Chapter 'Reconciliation and Developing Public Trust in Hungary: Opening State Security Files' in this volume.

because of the costs and significant delays involved in bringing cases to court. The courts are also often deferential to agencies, especially in matters relating to national security information.

*Duty to Publish Information*

A common feature in most FOI laws is the duty of government agencies to routinely release certain categories of information. This can reduce the administrative burden of answering routine requests and generally promotes openness.

Newer FOI laws tend to prescribe a listing of information. Under the Estonian Public Information Act, national and local government departments and other holders of public information have the duty to maintain websites and post an extensive list of information on the Web. They are also required to ensure that the information is not 'outdated, inaccurate or misleading'. In Slovenia, the Ministry of the Information Society sets regulations on what records a public body must publish. In South Africa, public and private organisations must publish manuals describing their structure, functions, contact information, access guides, services and a description of the categories of records they hold. The Human Rights Commission is required to create a guide based on the manuals.

## National Security and Freedom of Information

Nearly all countries have laws relating to the protection of national security-information. As noted above, freedom of information laws typically include an exemption for information relating to national security, a concept which is defined differently in various countries. In addition, many countries have State Secrets or Official Secrets Acts or provisions in their criminal codes which set limits on the release of information and criminalise its unauthorised release. Finally, a more recent trend is for countries, especially in Central Europe and Asia, to adopt laws on the protection of classified information that set out in more detail the types of information to be protected as well as the nature and duration of its protection. Many have also adopted laws on access to the secret police files of previous communist governments.

There is often a conflict between these laws and freedom of information. FOI acts generally create a presumption that information should be made public. These broad exemptions to access frequently raise serious concerns about the role of intelligence agencies, including in some of the most long-standing democracies. Ensuring national security is important to all nations but the balance is frequently skewed.

*FOI Exemptions*

Every national law on freedom of information and most sectoral laws have an exemption that allows for the government body to not release national security related information in its possession. The scope of the exemption varies but in

almost all countries national security is given the highest level of protection. In some countries, such as the United Kingdom and India, the intelligence agencies are excluded completely from the FOI law.[26] Often, the national security information such as that about an intelligence bodies' activities is presumptively kept secret even if it is not held by the intelligence service.[27]

Most countries provide the courts with some ability to review documents and decisions on secrecy. However, even when there is oversight, such as in the United States, the courts are often deferential to an agency's decisions (Blanton, 2003).

A few countries allow access to some information on the basis of harm potentially having been caused, such as the Bosnia Freedom of Information Act, which requires 'substantial harm'. The Peruvian Law on Transparency and Access to Information stipulates that information can only be withheld if it would 'cause a threat to the territorial integrity and/or survival of the democratic systems and the intelligence or counterintelligence activities of the [intelligence service]'. In the Peruvian case, journalists and senior military officers met and agreed to common definitions of national security and the types of information that could be withheld. Other laws may create specific categories of information that cannot be classified. Under the Mexican Federal Transparency and Access to Public Government Information Law, information relating to 'the investigation of grave violations of fundamental rights or crimes against humanity' may not be classified and all departments must produce a regular index of all classified files, which is subsequently made public.[28] In Bulgaria, the Prime Minister by executive order in 1994 decreed that the secret police files of the communist-era were to be declassified.

*Official Secrets Act*

Nearly all countries in the Commonwealth (the association of former colonies of the United Kingdom) have Official Secrets Acts (OSAs). These are typically based on UK law, often the original 1911 Act adopted by the United Kingdom and since partially repealed.[29] The Acts generally prohibit the release of any government information without permission. Often they also prohibit the further redistribution of information that is considered secret by other actors such as the media.

Typically, the recently adopted FOI laws override the OSA prohibitions on release of information except in the case of national security information. In New Zealand, the government repealed the OSA when the Official Information Act (an FOI law) was adopted in 1982.

---

26. UK Freedom of Information Act 2000, para. 23, India, Freedom of Information Act 2003, para. 16 and Schedule.
27. UK Freedom of Information Act 2000, para. 23.
28. Federal Transparency and Access to Public Government Information Law, available at http://www.freedominfo.org/reports/mexico1/laweng.pdf.
29. See for example India, Official Secrets Act, 1923.

*Classified Information and State Secrets Acts*

Many countries around the world have adopted laws that set out procedures on the classification and declassification of information. New members of NATO have adopted laws on protection of classified information (see below). Most Commonwealth of Independent States countries have adopted laws on state secrets based on the 1994 Russian State Secrets Act. In the United States, an executive order which has been changed or amended by each new President has been in place for over 30 years.[30]

*Categories* Most state secrets and classified information laws create a hierarchy of categories of security. Secrets are typically divided into levels of 'Top Secret', 'Secret', 'Confidential', and 'Restricted' or 'For Official Use'. Each level sets different thresholds for access, use and protection.

*Types of Information Covered* Many of the laws in question set out broad areas which include military and intelligence but also often scientific and economic concerns, which only have a tangential relationship to national security. The Czech Republic law takes a very broad view of classification and defines it as information 'which could cause detriment to the interests of the Czech Republic'including issues such as 'state material reserves', 'measures taken by customs authorities' and 'banking operations and the capital market'.[31] Many of the CIS countries' laws allow for the classification of information created and held by private bodies.

The US Executive Order 13,292 sets out eight areas that are eligible for classification:

(a) military plans, weapons systems, or operations;
(b) foreign government information;
(c) intelligence activities (including special activities), intelligence sources and methods, or cryptology;
(d) foreign relations or foreign activities of the United States, including confidential sources;
(e) scientific, technological or economic matters relating to national security, which includes defence against transnational terrorism;
(f) United States government programmes for safeguarding nuclear materials or facilities;

30. Executive Order 13,292. Further Amendment to Executive Order 12958 Classified National Security Information, March 28, 2003. Also see Ireland Freedom of Information Act, section 24; Canadian Access to Information Act, section 15; Bulgarian Law for the Protection of Classified Information, Appendix No. 1 of Article 25.
31. The Protection of Classified Information Act, Czech Republic 148/1999.

(g) vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to national security, which includes defence against transnational terrorism; or
(h) weapons of mass destruction.

*Duration* Typically the Acts set limits on the length of time that information should be classified. The duration typically in older acts and those in the former Soviet states ranges from thirty to fifty years. It is generally recognised that information should only be classified for the period in which the harm in withholding it is greater than the public good in releasing it. In practice this has not been particularly successful. More recent Acts have started to tie the level of classification into the duration and set shorter limits on the maximum duration of classified information of ten to twenty years. The US Executive Order sets a default of ten years unless it can be shown that a longer duration is necessary.

*Oversight* Under many of these acts, a specialised body is created which makes decisions on the categories of information to be classified and provides vetting of those who are authorised to access classified information. They can also review decisions on classification. In Hungary, under the Secrecy Act of 1995, the Parliamentary Commissioner for Data Protection and Freedom of Information is entitled to change the classification of state and official secrets.[32] In the United States, the Information Security Oversight Office is currently reviewing the decision by the Pentagon to classify the report on torture by military and civilian employees in Iraq.[33]

*Limitations* These laws typically place limitations on the types of information that can be classified excluding human rights violations, violations of other laws, and information relating to environmental hazards. The US Executive Order states that information cannot be classified in order to:

> conceal violations of law, inefficiency, or administrative error; prevent embarrassment to a person, organisation or agency; retain competition; or prevent or delay the release of information that does not require protection in the interest of the national security.

It also prohibits basic scientific information not clearly related to national security from being classified. The Slovenian Protection of Classified Information Act prohibits the classification of information relating to crimes.[34]

32. Hungary, Act LXV of 1995 on State Secrets and Official Secrets. See also Chapter 14 'Reconciliation and Developing Public Trust in Hungary: Opening State Security Files' in this volume.
33. See FAS Secrecy, May 7, 2004.
34. Article 6, Classified Information Act, Slovenia.

*New Laws, NATO and FOI*

The new Acts on the protection of classified information, which many countries in Central and Eastern Europe have been adopting as part of the process of joining NATO, have troublesome consequences for the freedom of information. Many of these countries were just leaning to develop a culture of openness when the NATO requirements were adopted. There was heavy pressure to adopt these laws under the threat of rejection from NATO membership and this resulted in little public or parliamentary oversight or discussion (Roberts, 2003). At the same time, NATO refuses to make public the standards that they are requiring the countries to adopt. The new laws frequently apply a very restrictive view of the disclosure of information that goes beyond files from NATO. In Bulgaria, the 2002 Classified Information Law eliminated the Commission on State Security Records that regulated access to, and provided procedures for, the disclosure and use of documents stored in the former State Security Service, including files on government officials.

*Specialised Laws on Access*

A number of countries have adopted specialised laws on specific areas where there is classified information that is of strong interest to the public. Following the transition to democracy, many Central and Eastern European countries adopted laws to address the issue of the files of former secret police forces. These files are made available to individuals so they can see what is being held on them. In other countries, access to the files is limited to 'lustration' committees to ensure that individuals who were in the previous secret services are prohibited from being in the current government or that, at least, that their histories are on record.[35]

The most advanced law on access is in Germany. Since 1991, a law allows individuals and researchers access to the files of the Stasi – East Germany's former security service.[36] The law created a Federal Commission for the Records of the State Security Services of the Former German Democratic Republic (the Gauck

35. See Hungary. Act XXIII of 1994 on the Screening of Holders of Some Important Positions, Holders of Positions of Public Trust and Opinion-Leading Public Figures, and on the Office of History, available at: http://www.th.hu/html/en/torv.html; Lithuania, Law on Registering, Confession, Entry into Records and Protection of Persons who Have Admitted to Secret Collaboration with Special Services of the Former USSR. No. VIII-1436. November 23, 1999. As amended by June 13, 2000; No. VIII-1726, available at: http://www3.lrs.lt/cgi-bin/getfmt?c1=w&c2=123807.

36. Act Regarding the Records of the State Security Service of the Former German Democratic Republic (Stasi Records Act) of 20 December 1991. Federal Law Gazette I 1991, p. 2272, amended by the First Stasi Records Act Amendment of 22 February 1994 (Federal Law Gazette I, p. 334), the Second Stasi Records Act Amendment of 26 July 1994 (Federal Law Gazette I. p. 1748), Article 12 Paragraph 22 of the Act of 14 September 1994 (Federal Law Gazette I, p. 2325), Third Stasi Records Act Amendment of 20 December 1996 (Federal Law Gazette I, p. 2026), as well as Article 4 Paragraph 2 of the Act of 26 January 1998 (Federal Law Gazette I 1998, p. 164).

Authority), which has a staff of 3,000 piecing together shredded documents and making files available.[37] There have been two million requests from individuals for access to the files and three million requests for background checks since the archives became available in 1991. Researchers and the media have used the archives 15,000 times. The German Federal Court ruled in June 2004 that there should be access to the files on former Chancellor Helmut Kohl, which may contain information related to illegal activities by Kohl while he was head of a political party. [38]

Other countries have provided for more limited access. In April 1996, the Czech Parliament approved a law that allows any Czech citizen to obtain his or her file created by the communist-era secret police (StB).[39] In March 2002, President Havel signed legislation expanding access to the police files of the communist regime to allow any Czech citizen over 18 years old to access nearly any file.[40] The government published a list of 75,000 StB collaborators in 2003 on the Ministry of Interior's website.[41] In Romania, the 1999 Law on the Access to the Personal File and the Disclosure of the *Securitate* as a Political Police allows Romanian citizens to access their *Securitate* (secret police) files.[42] It also allows public access to the files of those aspiring for public office and other information relating to the activities of the *Securitate*. A National Council for the Search of Security Archives (CNSAS) administers the archives.[43] Similar laws have been adopted in Slovakia and Bulgaria (since repealed by the Classified Information Act).[44]

In France, a 1998 law sets rules on classification of national security information.[45] The *Commission consultative du secret de la défense nationale*

37. Available at: http://www.bstu.de/home.htm.
38. Court orders release of Stasi files on Kohl's political life, *The Guardian* (UK), 24 June 2004.
39. Act N. 140/1996 Coll. of 26 April 1996 on Disclosure of Files Established by Activities of the Former State Security Force, Czech Republic.
40. Act 107/2002 amending Act No. 140/1996 Coll. on providing access to volumes created within the activities of the former State Security, and some other Acts, Czech Republic.
41. Radio Prague, Czechs wait thirteen years for official names of secret police collaborators, 24 March 2003, available at: http://www.radio.cz/en/article/38934.
42. Law No. 189/7 December 1999 on the access to the personal file and the disclosure of the Securitate as a political police, http://www.cnsas.ro/legeng.htm. See Ioana Borza, *Decommunization in Romania: A Case Study of the State Security Files Access Law*, available at: http://www.polito.ubbcluj.ro/EAST/East6/borza.htm.
43. Available at: http://www.cnsas.ro/indexeng.html.
44. For Bulgaria, see the Access to Documents of the Former State Security Service Act and Former Intelligence Service of the General Staff Act, 1997.
45. Loi no 98-567 du 8 juillet 1998 instituant une Commission consultative du secret de la défense nationale, available at: http://www.legifrance.gouv.fr/WAspad/UnTexteDeJorf?numjo=DEFX9700140L See Rapport 2001 de la Commission consultative du secret de la défense nationale, available at: http://www.ladocumentationfrancaise.fr/brp/notices/014000754.shtml.

(CCSDN) gives advice on the declassification and release of national security information in court cases. The advice is published in the Official Journal.[46]

In the United States, the Congress has enacted two specialised laws on access to files held by government agencies including the intelligence services and relating to the Assassination of President Kennedy (JFK Act)[47] and to Nazi and Japanese war crimes.[48] A third law on human rights abuses third countries is still being discussed. Both Acts created review boards to collect and examine documents and decide on their release. Over four million pages were released under the JFK Act, including thousands of previously classified records.[49] Over eight million documents have been released under the war crimes laws.

**Problems with Secrecy**

The costs of not making information available cannot be underestimated. These include both direct costs for the keeping of information and the indirect costs in efficiency and government credibility.

*Monetary Costs*

Classified information imposes significant burdens on public authorities to securely create and maintain the information. The US Information Security Oversight Office lists a number of areas where costs are impaired:

- Personnel security;
- Physical Security;
- Information Security;
- Professional Education;
- Security Management and Planning.

In the United States, the estimated cost of classified information was $4.7 billion in 2001, not including the CIA, which classifies the cost estimates of classification.

*Indirect Costs*

- Excessive classification can lead to political manipulation by those in charge of the files. Files can be selectively released to support and position. Recently, President Bush chastised Attorney General John Ashcroft for declassifying a document on the intelligence use of intercepted

46. For a copy of decisions, available at: http://www.reseauvoltaire.net/rubrique387.html.
47. President John F. Kennedy Assassination Records Collection Act of 1992.
48. Nazi War Crimes Disclosure Act. Public Law 105–246; Japanese Imperial Government Disclosure Act of 2000 December 6, 2000.
49. Assassination Records Review Board, 1998.

communications in an attempt to discredit one of the Commissioners on the panel investigating the reasons and failures of 9/11.[50] Meanwhile, documents released to Congress on whistleblowers were reclassified. Senator Patrick Leahy testified that 'Documents have been classified, unclassified and reclassified to score political points rather than for legitimate national security reasons'.[51]

- Classification is often used to hide embarrassing information rather than dealing with the core information necessary to protect national security. This became apparent recently when the families of a bomber crew that crashed in 1948 in the United States were denied access to the records and even to the courts under the reasoning that this posed a threat to national security. The resulting Supreme Court case, which implicated the entire system of national security limits on information in the United States, discovered that the files had been automatically declassified last year and revealed that the Air Force had not fixed known flaws in the bomber and had lied to the court about the information.[52] In Malaysia, the Air Quality Index, which reveals how polluted the air is – a very important issue in Malaysia where illegal burning and logging is endemic and government actions to prevent it have been limited – is withheld by the government as a secret under the Official Secrets Act. In the United States, the combined yearly budgets of the intelligence agencies going back to 1947 are considered classified information.

- It is also used to hide abuses and corruption. In Africa, the fight against corruption in Nigeria is hindered by government officials refusing to reveal to the public and members of parliament information about their activities because of claims of official secrets even when they have nothing to do with national security activities. It also hides abuse, such as interference in the domestic political system and the pressuring of government opponents by intelligence and law enforcement agencies. The United Kingdom prohibits individuals, including current Ministers and Members of Parliament, from accessing their own security files dating from when they were student protestors in the 1970s, because of the fear of showing how pervasive the surveillance was at that time.

- Excessive classification leads to a weakening of the protection of important information as well as manipulation by insiders who can selectively release information illegally to support their positions. US Supreme Court Justice Potter Stewart noted in the *Pentagon Papers* case in 1971:

50. FAS Secrecy News, 30 April 2004.
51. Statement of Senator Leahy, United States Senate Committee on the Judiciary DOJ Oversight: Terrorism and Other Topics June 8, 2004.
52. See Materials relating to Reynolds v. US petition for rehearing at available at: http://www.fas.org/sgp/othergov/.

> When everything is classified, then nothing is classified, and the system becomes one to be disregarded by the cynical or the careless, and to be manipulated by those intent on self-protection or self-promotion.

The US Commission on Protecting and Reducing Government Secrecy stated:

> classified documents are routinely passed out to support an administration; weaken an administration; advance a policy; undermine a policy. A newspaper account would be incomplete without some such reference.

Often keeping files secret does not guarantee that they will not be released for political purposes. In Hungary, the file of the Prime Minister Peter Medgyessy was leaked in 2002 revealing that he had once worked for a branch of the intelligence services. In April 2003, many of the Slovene security files of the UDBA, the former Yugoslavian secret police, were published on a web site in Thailand by the Slovene Honorary Consul for New Zealand Dusan Lajovic. The documents were on over one million people including the officials, collaborators, and targets of surveillance.[53] A US prosecutor investigated who released the name of an undercover CIA agent married to former Ambassador Wilson, who discredited the administrations claims that Iraq had attempted to buy nuclear materials. In his investigation, the prosecutor conducted interviews including with President Bush and many of his high-level aides.

- Excessive classification prevents government agencies and those outside from learning important lessons from the information withheld. In South Africa, the secrecy around the decommissioning of its nuclear programme prevents other countries from learning its lessons and preventing proliferation, which can pose grave threats to the national security of many nations.[54]

- An excess of secrecy also imposes a cost on the agencies' ability to act effectively and recruit new employees. As noted by Canadian Professor Wesley Wark in a paper commissioned for the review of the Canadian Access To Information Act (ATIA):

> Without a strong foundation of public knowledge, the ability of the [security and intelligence] community to function effectively in the long run is hampered in all sorts of key areas, among them recruitment and retention of high quality personnel, acceptance of their role, access to knowledge, and the capacity to engage in dialogue with experts outside the intelligence community fence (Wark, 2001).

53. REF/RL Balkan Report, 25 April 2003.
54. See South Africa History Archive, 2002.

## Conclusion

The current trends on access to information are both positive and worrying. On the one hand, many countries are becoming more open. On the other hand, access is being undermined by existing and news laws on national security information. Important decisions are consistently moving towards international organisations, which have resisted becoming more transparent.

Effective oversight of intelligence services requires that information about their activities be made public. Many countries have an overly expansive view of national security that has little to do with ensuring the integrity of the nation. These laws and restrictions need to be reviewed so that important information is protected for the period that it is necessary while less important information is routinely released.

*This page intentionally left blank*

Chapter 14

# Reconciliation and Developing Public Trust in Hungary: Opening State Security Files

*László Majtényi*[1]

## Introduction

This chapter explores the role of intelligence oversight institutions through the experience of the Hungarian transition to democracy presenting a counterpoint to previously elaborated themes of parliamentary-y and executive-focused oversight. Hungary's first Commissioner for Data Protection first discusses the status of informational rights in Hungarian legislation before moving on to illustrate the potential limits of these norms using three relevant cases.

## Informational Rights and Hungary's Transformation to Democracy

In Hungary, informational rights[2] played a unique role in the inspiration and chronology of events that made up the 'constitutional revolution', the common term for the transformation from the communist political system to a democratic one. This revolution was accomplished without shedding any blood (and very few tears) because the single-party state practically collapsed under its own weight in 1989 after the demise of its foreign base of power. Due to the peaceful nature of the transformation, and in part because of the continuity of the old bureaucracy, there was the danger that some of the ingrained habits and relations of power of the former state would survive, and, as we have discovered, they certainly did. These characteristics of the process gave the new institutions and ideals special significance by imposing constitutional democracy on the whole of the state apparatus, as it were, from the outside. This is how informational rights emerged in Hungary as one of the key elements in establishing a liberal democracy. The establishment of informational rights was a struggle for which the institutional

1. The author was Hungary's first Data Protection Commissioner from 1995–2000.
2. This term refers to the legal arrangements designed to ensure the protection of personal data and public access to information.

background was provided by the first Constitutional Court[3] and then by the Office of the Data Protection Commissioner. These endeavours were supported by the ambitious and, at least during the early years, successful effort to fashion a constitutional order for Hungary. The objective was not simply to meet the internationally accepted bare minimum or even average standards for the protection of civil liberties, but rather to emulate the highest possible standards. Therefore, the advocates of informational rights set themselves the goal of replacing the informational policy of the single-party state, which favoured citizens transparent to an inscrutable state, with the reverse ideal: that of a state transparent to its inscrutable citizens.[4] It should be pointed out that overcoming the former state of affairs is a formidable hurdle not only for 'new democracies'. The rampant secrecy of government has been the nagging existential problem of every developed democracy since the earliest days of the constitutional idea itself (Armstrong, 1998), and the battle against such secrecy is one of uncertain outcome.

The political transformation made it possible to articulate society's informational needs in relation to the secret services as well. In 1995, the Hungarian parliament created the Office of the Data Protection Commissioner. During the first year of its existence, the Office was beleaguered by vague and contradictory regulations, a lack of legislation providing for national security, and more than one surviving statute issued by the *ancien régime*.[5] Parliamentary monitoring of the secret services,[6] as discussed below, was wrought by very basic difficulties. With few exceptions, practically every democracy runs secret services that are exempt from the general principle of 'transparent state – inscrutable citizens'. Nevertheless their control from the outside is not pointless, since agencies authorised to collect information in secret pose the risk of overstepping their law-given powers. This is precisely why they must be held accountable incessantly – by parliament, investigative journalism, and human rights activists. Secret services deserve our attention not only in terms of free access to information, but also with regard to the protection of privacy. On the one hand, this follows from their objective in the covert control of information, including personal data which is often sensitive in nature. On the other hand, the essentially secret manner in which they process information makes it impossible for outsiders

3. Whose President, László Sólyom, has himself been recognised as an expert of informational rights.
4. It is not the purpose of this study to examine Hungary's 'lustration' legislation and practice (that is, the background check on public officials), the fate of the documents created by the secret services of the single-party state, or the still unsolved set of problems surrounding the informational compensation of the previous regime's victims.
5. The National Assembly adopted Act CXXV of 1995 on the National Security Services on 19 December 1995. Except for a few provisions, the law entered into force on the 90th day following its promulgation.
6. In Hungary's constitutional system, the Office of the Data Protection Commissioner reports to the National Assembly. Based on the nomination of the President of the Republic, the Commissioner is elected by a two-thirds majority of the single-chamber parliament, for a term of six years.

to become familiar with their operations beyond a certain limited extent. Indeed, it is believed that the ongoing and efficient monitoring of these agencies by democratic institutions is practically impossible. This is suggested by a number of scandals over their activities that have erupted around the world. (Electronic Privacy Information Center; Flaherty, 1989; Adler, 1992).

*The Hungarian Data Protection Commissioner.*

In terms of the difficulties associated with efficient monitoring, the Data Protection Commissioner is in a somewhat privileged position having being vested with broad powers, including the right to inspect premises to determine the lawfulness of the data processing operations conducted there. At the same time, citizens with a complaint are often prevented from citing facts to support their claims, or even to help identify the organisation whose activities they wish to protest.[7] Received complaints disputing the practices of national security agencies suggest that the focus of interest is mainly on surveillance by concealed devices and covert methods. Most of these complaints, typically about being 'tapped' or 'under surveillance', do not even make it clear whether the culprit is a national security agency, or any of a number of organisations legally engaged in collecting covert intelligence.[8] Moreover, it is often beyond the Commissioner's powers to prove surveillance, as such, illegal. In such cases, then, what normally occurs is that the citizen concerned is told to contact the organisation in question as the first step, and then to return with the complaint only if they do not deem that answer they get to be satisfactory.

The cases described below, however, demonstrate the ability of the Commissioner to exercise a certain amount of control over the secret agencies. Nevertheless, this does not change the fact that, lacking proper investigative powers and a staff specialised in dealing with the secret services, such control will remain drastically limited in scope.[9] While the Commissioner is entitled to inspect secret files, his lack of proper investigative power means that he is confined to those documents that the organisation under review has actually supplied to him.

On a positive note, the Commissioner is authorised by law to supervise the process of classification of information and, as part of these powers, to recommend documents for declassification; this is a unique provision compared with other countries. In this context, the Commissioner's jurisdiction certainly goes beyond the scope of influence normally accorded to an ombudsman's office. Under law,

7. In Hungary, about a dozen organisations are entitled to collect information in secret, including the national security service, the police, the border guard, the tax authority, and the finance guard.
8. Hungarian Data Protection Commissioner, cases 254/A/1997, 537/A/1997, 709/A/1997.
9. In Hungary, a nation of ten million, the staff of the Data Protection Commissioner has never exceeded twenty. This is a hopelessly small number of employees to exercise continuous control over a wide range of data controllers, including direct marketing businesses, health care institutions, banks, insurance companies, the police, and the armed forces.

the classifier has no choice but to either accept the commissioner's advice or to challenge it in the Budapest Municipal Court. However, one ought to note that none have taken such action, choosing rather to concur grudgingly with the Commissioner's recommendation to discontinue or ease the classification in question.

**Judicial Checks on the Secret Services**

For a brief overview of this topic, it is essential to bear in mind that in Hungary's constitutional system, neither the general ombudsman nor the Data Protection Commissioner[10] has the right to criticise court decisions.[11]

These limitations notwithstanding, submissions by a Hungarian judge and a few claimants gave the author the opportunity to examine constitutional problems caused by the limited access to the information practices of the national security services. In lawsuits over the way such services handle data, it should be essential for the courts to be familiar with the objectionable activity that is at the crux of the civil litigation. In reality, however, effective regulations do not guarantee the courts the scope of inspection that would be necessary in such cases. As a result, the lack of sufficient information prevents the courts from being able to decide such disputes.[12]

In a remarkable incident, the Commissioner was contacted for advice by the presiding judge of the Budapest Municipal Court. The judge explained that the plaintiff in the case – an ordinary citizen – had requested that the Security Service's Information Office, the defendant, allow him to inspect the files kept on him and to discontinue the unlawful processing of his data by deleting him from the records. The Office turned down this request, citing the interests of the interior and exterior security of the state as a justification recognised under the Data Protection and Freedom of Information Act (the DP&FOIA), and insisting that it 'is not engaged, nor has it been engaged, in any illegal processing' with regard to the claimant's data. The Information Office cited section 44 of the Act on National Security Services 1995 (Hungary) to support its refusal to release pertinent information to the court itself. The provision quoted is as follows:

> (2) The Police, the Border Guards, the Customs and Excise Office, the courts of justice, the public prosecutor's offices, and the organs in charge of penal institutions are entitled to request data from the national security services, indicating the specific purpose thereof, to fulfil their tasks specified in the relevant Acts, within the scope defined therein. (3) The supply of data by the national security services may not result in the disclosure of the person co-operating with the national security services

10. Nonetheless, the Data Protection Commissioner is entitled to inspect the court's habits of processing information.
11. The best counterexample is provided by the Scandinavian countries, where the ombudsman is normally authorized to critique the courts (Majtényi, 1992; Al-Wahab 1983; Hiden 1973).
12. Hungarian Data Protection Commissioner, case 800/K/1997.

> (the sources data). In order to protect the method and source of intelligence gathering, the Directors General of the national security services may impose restrictions on the use of the data delivered.

The presiding judge contacted the author with reference to section 26 of the DP&FOIA, under which the Commissioner's powers of document inspection are broader than those of the courts:

> In exercising his functions the Data Protection Ombudsman may request that the Data Controller furnish him with information on any matter, and may inspect any documents and records likely to bear on personal data or data of public interest. [...] State and official secrets shall not prevent the Data Protection Ombudsman from exercising his rights stated in this Article, but the provisions on secrecy shall bind him as well. In cases affecting state or official secrets the Data Protection Ombudsman shall exercise his rights in person …

The case raised a number of legal dilemmas:

- Section 50 (1) of the Constitution declares that: 'The courts of the Republic of Hungary protect and guarantee constitutional law and order as well as the rights and lawful interests of citizens, imposing punishment on the perpetrators of crimes'.
- Identifying the tasks of the courts, section 141 (5) of Act III of 1952 on the Rules of Civil Procedure provides that 'the presiding judge shall refer to such documents and other information as may be available and proceeds, to the extent this is necessary for ultimately deciding the suit, to summon the parties and witnesses for the scheduled court date and to obtain further documents serving as evidence in the case'. Section 119 of the same Act generally prohibits parties, prosecutors and other participants in a court case from making copies or abstracts of documents barred from public inspection for reasons of secrets of the state, office, or business. In fact, the mere inspection of such documents is subject to special conditions established by the presiding judge. In contrast, the quoted provisions of the National Security Act in effect prevent the courts from fulfilling their constitutional and legal function by reaching a well-founded decision in the informational dispute between the citizens and the services.
- Based on the Act on Parliamentary Commissioners and the DP&FOIA itself, the Data Protection Commissioner may not legally conduct an investigation into a case already in court, whereas the court is unable to reach a verdict for lack of sufficient information. As the Commissioner in office at the time, the author declined to voice his position in this particular case. The Minister who did not possess a portfolio for overseeing the national security services was contacted and agreed that the lack of sufficient safeguards prevented the presiding judge from speaking out on

> the legality of the data processing in question, other than to conclude that the services had indeed acted within the law.[13]

In short, both the law and the policy of the national security agencies barred the acting judge from accessing the facts of the case. Under the circumstances, the intervention of the Commissioner had to be confined to warning legislators and those applying the law of the law of the unacceptable constitutional impasse. It is unacceptable that in the case of the secret services infringing upon privacy that the law guarantees the right for a judicial check but it does not guarantee any right to the judge to know the state of affairs. The problem has remained without a constitutional solution to this day. But, after all, the test of efficient legal protection is not words or goodwill but investigations that produce tangible results. Let us therefore look at a few relevant cases.

## The Role of the Data Commissioner in Practice

The following three cases have been selected to give an impression of what the Data Commissioner is able to achieve. The first case tested the legal limits on secret service surveillance of Hungarian citizens. The second case dealt with modalities of classification and checks against its abuse. Finally, the third case considered the question of the improper documenting of closed government sessions.

### *Illegal Surveillance of Civilians (1990–1995)*

The first significant debate with the central administration over illegal data collection practices of the secret services erupted in 1995, the year the author was elected Commissioner. It was started by a member of parliament who requested an inquiry into security checks conducted by the Bureau of National Security (the Bureau) as part of an integrated process from 1990 to 1995.

Serving as Commissioner, the author therefore examined the legality of security checks ordered between 1 May 1990, and 31 March 1995. He found that almost every one of the 797 checks conducted in this period were illegal. The services involved volunteered the information that the intention was to run background checks on persons nominated for public service, but these persons were not advised about the facts or the purpose of these checks. To make things worse, the cited purpose turned out to be disingenuous in a significant portion of the cases.

The purpose of the checks went mostly without mention in the files, while in 138 cases the order for the check was issued verbally. In fact, it was often impossible to determine where the orders had come from. Although in a few of the cases involved the suspicion of a felony having been committed, it remained

13. Hungarian Data Protection Commissioner, case 800/K/1997.

unknown whether the Bureau forwarded such information to the investigative agencies. The orders for the checks were also inconsistent, considering that some employees were subjected to them, while others of the same rank within the given organisation were not.

The Bureau often ran checks on persons, including businessmen, journalists, and politicians, who clearly did not hold nor ran for particularly important or confidential positions. The Commissioner suggested that the checks raised further concerns in terms of the Constitution, privacy and criminal law, and that they wanted these issues clarified.

The Minister responsible accounted for the surveillance in a letter, which he chose to classify as a state secret, by noting that such checks were founded on a regulation stating that collecting information is legal if it 'serves to protect persons holding particularly important and confidential positions, and provided that these persons are aware that information is being collected on them'.[14] While it was impossible to say precisely how many of the 797 subjects were aware of the checks, it became apparent that they were generally not informed.

The checks were typically ordered – often only verbally – by the Minister without portfolio, and occasionally by the cabinet chief or the General Director of the Bureau. If the entity ordering the check prepared a transcript, these normally contained data on the individuals to be checked, but did not say whether or not the person was informed about the check or what the purpose of the check was. According to the instructions of the General Director, the documents were filed locally by the department conducting the checks.

The investigators of the Bureau of National Security went through all the files they could obtain, including the records of the military and civil national security services, the population census database, and those criminal and alien records of the Ministry of the Interior and the National Police Headquarters that were accessible to the Bureau. They also made use of various public databases maintained by government agencies, and often compiled reports on the subjects as well.

In the investigators assessment, security risk factors included lack of loyalty to the sovereignty and constitutional system of the Republic of Hungary, legal violations, major flaws and distortions of moral character, addiction, excessive debt, financial instability, sexual misconduct, serious psychological disorders, and undesirable foreign relations.

Evidently, some of the checks were not motivated by considerations of national security. It was clear that many individuals were subjected to checks without a well-founded legal reason. Due to the limitation of the Commissioner's powers, the inquest was unable to identify explicitly the real intention of these security checks. The lack of certainty notwithstanding, there were reasons to suspect political motives behind these illegal checks.

The violations brought to light were also related to shortcomings and gaps in the regulations, as well as to the lack of legal and political closure in the wake of

14. Decree of the Council of Ministers 26/1990 III.14.

the political transformation. However, even the provisions in effect at the time stipulated the subjects' awareness as a precondition for using special methods. Consequently, the greatest wrong committed by the services was that they habitually neglected to inform the subjects, before or after collecting information on them.

First and foremost in the recommendations made, the Minister was urged to declassify his letter as it contained nothing to justify its categorisation as a state secret. Incidentally, the classification note was not signed by the classifier, and thus the letter could not have been regarded as a state secret to begin with under the provisions of the Secrecy Act.[15] Next, the Directors of the secret services were called on to inform the subjects of the security reports and the fact that information was collected on them, and to apologise for the violation. This obligation could be waived only if it could be shown that the subject had been informed on a previous occasion. The information had to be communicated thus showing full respect for the individual rights of the subject of surveillance and any third parties that might have been involved. It was also suggested that the subjects be given the option to have their files destroyed, unless the check could be proven to have been legal. The Minister concurred with these recommendations and all the subjects were eventually notified.

*Excessive Secrecy*

*Facts of the Case* Act CXXV of 1995 assigns to the national security services the duty of uncovering operations that threaten the economic interests of the country. On account of its strategic importance, the oil trade had been continuously monitored by the Bureau of National Security. Moreover, a parliamentary investigative committee had been established to investigate abuses related to deliveries of Russian oil as payments on Russia's outstanding national debt to Hungary. On 16 December 1996, the Data Protection Commissioner was requested to provide a position to 37 members of parliament who protested the decision of the Minister to classify as a state secret – for a period of 80 years – his letter answering questions posed by the parliamentary investigative committee. The parliamentarians argued that:

> The investigating committee can only make its findings public if the information obtained is prevented from being shelved in national security archives for generations.

The petitioners – most of whom did not serve on the committee and therefore had no access to the letter – expressed their doubts as to the existence of any interest expressly defined under section 3 (1) of the Secrecy Act that might justify the classification of the letter, and requested the Commissioner to call on the Minister to remove or at least to alter the terms of the classification.

15. Act LXV 1995, Section 7.5.

The Minister was asked to explain his position as well as the reasons and legal grounds for his decision. In his response, the Minister addressed issues pertaining to the legal grounds of the classification as well as its conformity in terms of both form and substance. He explained that, according to the Secrecy Act (section 3), state secrets included data categorised in the groups specified in the appendix to the Act – the disclosure of which prior to the expiry of the validity period, as well as its unauthorised access, use or transfer to an unauthorised third party – would violate or threaten the national security interests of the Republic of Hungary. Based on the List of State Secret Categories,[16] the quoted appendix to the Act, the maximum period of secrecy classification is 80 years for data pertaining to the acquisition, analysis, processing and use of information necessary for the proper functioning of the government in foreign policy, economic, defence or other crucial interests of the Republic, as well as for data relevant to the organisation and practice of activities furthering its interests.

The Minister also addressed the assumption that while the act of classification itself might have been legal, the requested period of classification was completely unacceptable. The Minister pointed out, however, that the law invested him with a 'rather broad scope of discretion', and that it was both his right and duty to protect data for as long as he saw fit. While the duration of classification often could not be correctly assessed at the time it was assigned, once it had been specified it could not later be modified by the classifier in this category of information.

Nonetheless, section 10 of the Secrecy Act required the classifier to review the decision every three years and to declassify the document if the circumstances justifying the original classification no longer existed. Considering all this, the Minister insisted that he had acted in the spirit of the law, satisfying both formal and substantial requirements. He also pointed out that the disputed classification could not be judged out of context as the letter was merely one in a series of documents related to the case in question. In support of his argument, the Minister sent a copy of the letter that had been classified and pledged further information to help for a better understanding of the case.

*Legal Considerations* Section 61 of the Constitution declares that everyone has the right to access and disseminate data of public interest. Freedom of information legislation in Hungary requires a two-thirds vote of parliament to pass, considering that what is at stake in such legislation is one of the pillars of constitutional democracy. The DP&FOIA of 1992 provides for the scope of freedom of information and the terms of its restriction. Section 19 of the DP&FOIA articulates the general mandate for agencies and officials of the central and local governments, as well as other institutions and individuals performing public functions, to promote the prompt supply of accurate information to the general public in matters under their respective jurisdictions. These agencies no doubt include the national security services and parliamentary committees, permanent or

16. Clause 101 of the List.

ad hoc. Like other public bodies, they must periodically publish the most important data concerning their activities. As it derives from the Constitution itself, this universal legal obligation cannot be waived with reference to categories of secret or non-public data, documents for interior use, business secrets, tax secrets, banking secrets, etc. – whether defined by the Secrecy Act or other regulations. Freedom of information is not an absolute liberty, and as such it is subject to restriction. This means that access to data of public interest may be restricted if ordered by law, for instance by a state secret classification – of course, without prejudice to the guiding principle of informing the general public. Although section 19 (3) of the DP&FOIA states that access to data of public interest may be restricted in the interest of national security, the question of to what point that restriction may be lawful must always be answered on a case-by-case basis.

The relationship between the Secrecy Act and the DP&FOIA must be seen in light of the general rules of restricting a fundamental right, but also in terms of the rules of these two Acts themselves. The need for secrecy *vis-à-vis* the right to freedom of information must always be interpreted restrictively. This follows from section 8 (2) of the Constitution and the interpretation of that paragraph by the Constitutional Court. A fundamental right may not be restricted in its essential substance even by an Act of parliament. The restriction cannot be lawful unless it meets the criteria of equity, is confined to a bare minimum of necessity, and allows for the exercise of the fundamental right. The interests of national security – although they are not spelled out as such in the language of the Constitution – are recognised as important constitutional interests by the DP&FOIA and in the Commissioner's appraisal (this interpretation is supported by an analysis of the rulings of the Constitutional Court).[17] These interests, however, must take second place to fundamental informational rights in the hierarchy of constitutional privileges. This reading in turn can be demonstrated to be correct by comparing section 1–4 of the Secrecy Act with section 19 of the DP&FOIA. While the DP&FOIA orders the 'prompt and accurate information of the public', the Secrecy Act merely talks about 'data' or 'types of data' that may be barred from public access.

Even if certain data may be legally concealed, this does not affect the universal mandate to inform the public. This interpretation is in line with the role of the national security services to protect the Constitution. In a lucid and rather precise usage of the Secrecy Act, the justification of a 'state secret' is not the interest of the 'state' so much as it is the interest of the 'Republic of Hungary'. The meaning of the 'Republic of Hungary' is not one agency or another, but the community of citizens.[18] Considering all this, recommendations were made by an

17. 34/1994 (VI. 24.) building on the argument of 30/1992 (V. 26.), and 60/1994 (XII. 24.).

18. Section 3 (1) 'State secret means any data of the type defined in the Appendix to this Act (hereinafter: state secret categories), which has been classified in due procedure by an authorised person who has established beyond the shadow of a doubt that, before the lapse of the classification, the disclosure, unauthorised possession or use of the data, or its disclosure to an unauthorised person or withholding from a person

aide to the Minister that departed from the suggested approach, and proposed that the government's classifying practices and related individual cases could not properly be assessed based merely on two or three provisions taken out of the Secrecy Act, but only in the context of other laws and the Hungarian Constitution. It was therefore arguably wrong to construe the Commissioner's job here to hold this matter to the test of the Secrecy Act alone, but rather to examine it also in the light of the DP&FOIA, which incidentally provides for the tasks of the Commissioner as well. The Secrecy Act is part of the entire legal system as surely as the secret services and the ministry in charge of them are part of the democratic system of government.

If significant parts of a document contain data that can be regarded as state secrets, then the entire document may be legally classified. However, in case of a number of related documents, such as correspondence between various institutions, each document must be considered separately. In other words, a document cannot be legally classified simply because it was created, for instance, in answer to a letter that had been labelled, rightly or wrongly, as 'Strictly Confidential'. In short, each document must in itself meet the legal criteria before it can be properly classified. Section 25 (1) of the DP&FOIA provides that:

> The Data Protection Ombudsman shall monitor the conditions for protection of personal data and for disclosure of data of public interest [...] The Ombudsman may initiate a decrease or an increase in categories of data classified as state or official secrets.

Under section 26 (4):

> The Data Protection Ombudsman shall call the authority who classified the data for alteration or deletion thereof, if he considers the classification unreasonable. The authority may apply to the Capital City Court against the warning within 30 days of the notification thereof. The Court shall conduct the proceeding in camera and with special dispatch.

This latter provision vests the Commissioner with power in excess of the rather 'mild' authority normally accorded to ombudsmen.

Another circumstance that had to be considered in the case of oil-sales to Russia was the period of the classification. The Minister was clearly out of line when he claimed that the law conferred upon him 'a rather broad scope of discretion' in defining the duration of the classification, for such scope of discretion could not be regarded as limitless within the time frame allowed by law.

The dialogue between state and society serves to constantly renew the social contract between citizens and their government. The public bodies have no right to exempt themselves from public scrutiny. Section 26 (3) of the DP&FOIA provides

---

> entitled to access, would violate or jeopardise the interests of the Republic of Hungary pertaining to national defence, national security, criminal investigation and prevention of crimes, monetary and currency policy, international relations, or judicial procedure'.

that the classification of a document may not hinder the Commissioner's investigation, but the confidentiality will be binding for him as well. As a matter of course, the Commissioner has no right to divulge the contents of the document even if he happens to disagree with its classification. For this reason, the recommendation published in the case at hand had to be confined to stating that the disputed document was part of a longer series of communications, both verbal and written, whose major elements had all been classified as state secrets. The classification seemed justified in view of a few words and phrases that cropped up in the text, but the document was unsuitable, in its unabridged or edited form, for the information of the general public. All things considered, it was concluded that the classification itself remained within the law, even though the 80 years could be considered excessive. One could safely exclude the possibility that, several generations down the line, the Republic of Hungary will have any appreciable interest in keeping this data secret, just as it seemed safe to assume that the Russian oil fields in point that supplied Hungary's demand will have long been depleted by the time the proposed classification will expire.

*Implications from the Data Protection Commissioner* Instead of calling for the removal of the classification, the Minister was urged to meet the disclosure obligation with respect to those parts of the document that did not qualify as state secrets. Another legal alternative was to strip the document of the confidential data. It was also pointed out that the information released to the public had to be both serious and genuine. If the document was nevertheless kept from disclosure, this had no bearing on the right of citizens and organisations who felt wronged by the cover-up from seeking remedy from the National Security Committee of Parliament, the Data Protection Commissioner or – as a another option available under the DP&FOIA – from the courts themselves.

While in the recommendation of the Data Protection Commissioner the Minister's letter was not required to be declassified altogether, the following stipulations were attached:

- The classification of the letter for 80 years, the maximum period allowed by law, not only contravened the rules of both the Secrecy Act and the DP&FOIA, but also hindered the building of much-needed trust between society and executive power. The Minister was urged to review his decision and to reduce the validity period of the classification by a significant number of years.
- Data could not legally be kept from society unless it met the criteria of state secrets as defined in the Secrecy Act, other provisions of law, and in the interpretation advanced in the recommendation. The substantial findings of otherwise secret investigations were subject to disclosure, to the extent that they represented data of public interest. The relations maintained by political decision-makers and business interests that might be in violation or jeopardy of the Constitution must be regarded as data of public interest. It

> was the constitutional duty of the government, the secret services, and the parliamentary committees to inform society of such findings, to the extent that this was feasible without divulging state secrets. First and foremost, this information had to take the form of opening up the document for public inspection. If this was not possible, in part or in full, for some lawful reason, the substance of the document still remained subject to disclosure. The overriding interests of transparency and probity in public affairs made it unacceptable to restrict the publicity of proven abuses. In closing, it was noted that the negative outcome of the investigation or its lack of results also constituted information of public interest.[19]

Although the last case addressed here has no direct or visible implications on national security, it is tempting to see it as a symptom of the paranoia permeating constitutional democracy. As such, it is an apt illustration of the kind of perversion in government that may easily overflow the shadowy confines of the secret services to infect the whole apparatus of the state.

*Cabinet Sessions: On or Off the Record?*

The Data Protection Commissioner launched a probe into the issue of documenting sessions of the cabinet, including the preservation and disclosure of such documents after citizens had urged for this to be done. After the cabinet's rules of procedure were modified in June 1998, cabinet sessions were no longer audio-taped or otherwise recorded in verbatim minutes until the opposition emerged victorious in the 2002 elections. A look at the history of documenting cabinet sessions offers valuable lessons for the legal judgment of the case. The Hungarian National Archive keeps the documents of governments that served in 1848–1849,[20] 1867–1944, and 1944–1983. These records are now open for research and the Archive receives nearly a thousand requests for data annually from researchers wishing to study them. Changes in government practices with regard to documenting cabinet sessions and preserving those records can be traced with clarity over the years. The governments after the political transformation of 1990 returned to the habit of holding their sessions on the record. This constitutional routine was derailed by the above-mentioned procedural change,[21] instated by the government formed in 1998, which abolished the rule on documenting cabinet sessions.[22]

---

19 Hungarian Data Protection Commissioner, case 618/A/1996.

20. The age of modern parliamentary culture in Hungary, understood as government reporting to parliament, began with the fall of Habsburg absolutism in April 1848. From 1849, when the revolution and war of independence were crushed, until the Compromise of 1867, power reverted to absolutist models.

21. Government Decree 1090/1998 VII.15.

22. According to this regulation, which remained in effect until the ruling party lost the elections in 2002, 'The abstract prepared of sessions of the government shall contain the names of those attending, the titles of the proposals discussed, the names of those

When inspecting the administrative premises of the Office of the Prime Minister on 10 December 1998, the official heading the department stated that every proposal to be discussed by administrative secretaries prior to convening a session of cabinet was classified as 'Strictly Confidential', 'Confidential', or 'Not Public'. The classifying stamp was affixed by the administrative department itself if the document had been submitted to the Office of the Prime Minister without one of these designations.

Democracies around the world employ various means to document the operation of their governments. Some countries insist on verbatim minutes, while others merely mandate abstracts of content. Accordingly, there are many ways to regulate the process of recording and the handling of the documents thus created. In certain countries, freedom of information is a constitutional right; in others it is a privilege guaranteed by law only; in several countries, which lack proper legal regulations on this count, the need for this freedom is acknowledged and legitimised by custom and an unwritten constitutional code of values. In some places the preferred solution is to remove a specified range of government papers from the effect of freedom of information. Starting in the 18th century, monarchs often made the solemn pledge that the affairs of the state would be conducted in full view of the public eye.[23] The age of enlightened absolutism heralded a period in which the citizens' right to exercise control over government have gradually broadened, despite a number of setbacks in the process. This right also implies the publicity of the government's papers and of its operations.

Hungary's Constitution declares that:

> in the Republic of Hungary, every individual is granted the right to free expression, as well as to access and disseminate data of public interest (section 61.1).

Section 8 (2) states that:

> the rules of fundamental rights and obligations are set down in the law, which may not, however, restrict the essential substance of these fundamental rights.

Pursuant to section 2 (3) of the DP&FOIA:

> data of public interest means any information under processing by an authority performing state or local self-government functions or other public duties, except for personal data.

Section 19 (1) and (3) provide that:

> [the authority] performing state or local self-government functions or other public duties ... shall, within its sphere of competence, including its management, promote

---

contributing comments to the debate, the fact and for/against ratio of voting, if any, reference to the disagreement, if any, voiced by a cabinet member from the coalition party, as well as the decision itself'.

23. A case in point is the 1868 Imperial Oath taken by Japan's Emperor.

> accurate and prompt information for the general public. [...] The authority shall grant access for anyone to data of public interest processed by it, except for those data which are classified as state or official secret by authorities entitled to do so under provisions of law, furthermore provided that right to access of certain data of public interest is not specifically restricted by law in the interest of national defence, national security, criminal investigation and the prevention of crimes, monetary or currency policy of the state, international relations and relations to international organizations, or judicial procedure.

Section 19 (5) declares that:

> Unless otherwise provided by law, working documents and other data prepared for the authority's interior use, or for the purpose of decision-making, are not public within 30 years of their creation. Upon request, the head of the authority may permit access to these documents or data prior to the expiration of this period.

Pursuant to section 6 (1), clause o) of the Secrecy Act:

> In their respective scope of responsibilities and competence, [those] entitled to classify documents are the head of the Prime Minister's Office, the political secretary of the Office, and the head of the body operating according to the Rules of Procedure approved by the government.

The matter under review is rife with the difficulties inherent in reconciling a number of mutually conflicting constitutional rights and interests. The regulations must observe the constitutional right to access data of public interest. They must serve the cause of transparency in the work of the government, leave open the opportunity for the scholarly and scientific study of governments past and present, and they must be conducive to the smooth operation of the administration free of undue influence. In this sense, there are no constitutional grounds to demand full publicity of the entirety of the government's activities as a condition for the said smoothness of its operation.

The disclosure of data of public interest is a fundamental proof for the proper functioning of a democratic constitutional state as it is declared in section 2 (1) of the Hungarian Constitution. The significance of this was recognised in the Council of Europe's 1982 Declaration on the Freedom of Expression and Information, when it affirmed the goal of the member states to follow an informational policy of openness in the public sphere – including one of allowing access to information – in order to help their citizens to better understand political, social, economic and cultural issues, and to improve their skills in freely discussing such topics.[24] Nevertheless, the disclosure of data of public interest and the right to free research both encounter constitutional limits in those provisions of secrecy

24. Council of Europe, 'Declaration on the Freedom of Expression and Information', 1982. Clause 8. II. C. *Adopted by the Committee of Ministers on 29 April 1982, at its 70th Session*.

which comply with legal requirements and the rules governing the restriction of constitutional rights.

'The smooth operation of the administration free of undue influence' would obviously be thwarted if the law prescribed full publicity of the sessions of cabinet. Little wonder that this is not the custom in democracies around the world. Therefore, far from being illegal, provisional restrictions upon the freedom of information can be constitutionally well-founded when such restrictions are motivated by the above purpose. It could not properly be regarded as a constitutional exigency to prepare full documentation of cabinet sessions – that is verbatim minutes, audio and/or video tapes. The manner in which the sessions are to be documented can be legislated in several ways. One must bear in mind that the cabinet is not a congregation of private individuals, but rather a body of officials that plays a crucial role in the system of political institutions. On account of its prominent legal and political position, it is indispensable to have its activities documented, not simply to the extent of publishing its resolutions, but in terms of content and substance. Seen in this light, Government Decree No. 1090/1998 (VII. 15) clearly broke with the traditions of 1848 which had held sway for a century and a half in Hungary. The total prevention of access in the interest of 'the smooth operation of the administration free of undue influence' cannot be deemed inevitable or, for that matter, equitable.

The Commissioner for Data Protection and Freedom of Information concluded with the following recommendation:[25]

- The author called on the Minister heading the Prime Minister's Office and the Minister of justice to propose legislation documenting the substance of government sessions that would not only ensure the smooth operation of the government free of undue influence but also guarantee the citizens' constitutional right to access data of public interest – acknowledging that there may be delays in the enforcement of this right in individual cases;
- Documents classified with disregard for clause 13 of the Appendix to the Secrets Act could not properly be regarded as state secrets because they were not specifically identified as such in the effective list of state secret categories.

The government chose not to accept the author's recommendations.

25. For a full English-language version of Recommendation 144/A/1996, dated July 16, 1996, see the home page of the Office of the Data Protection Commissioner available at: http://www.obh.hu.

## Conclusion

As the above-mentioned cases imply, the Bureau of the Commissioner for Data Protection and Freedom of Information was probably one of the most active organs with regard to the external control of the secret services. With its highly limited means it has discovered numerous violations of law in connection with qualification of state secrets and the functioning of the secret services, and has laid these before the public. Although the Commissioner cannot issue any binding decisions, the high degree of respect for the Bureau of the DP&FOI Commissioner and the resulting publicity often forces the executive to accept its recommendations.

*This page intentionally left blank*

# PART VI

# Conclusion

*This page intentionally left blank*

Chapter 15

# Intelligence Services: Strengthening Democratic Accountability

*Hans Born and Fairlie Jensen*

**Introduction**

Democratic control is a particularly challenging task when it comes to intelligence agencies. There is a legitimate requirement for secrecy, that is, for restricting access to details of the operations of intelligence agencies. This imperative for secrecy, however, can be abused and may lead to inefficiency, unauthorised actions, or the misuse or politicisation of intelligence agencies. In such instances intelligence agencies can lose sight of ethical principles, evade political control, and even become a threat to the society and political system they are meant to serve. Public distrust of government secrecy has led to calls for some measure of oversight of intelligence structures. At the same time, these agencies must be able to perform the functions they are mandated to carry out. The need for democratic oversight of intelligence services is as necessary in mature democracies as in many of the Central and Eastern European countries whose intelligence services have been undergoing a process of reform. Countries in transition to democracy moreover must often deal with enduring legacies of repressive intelligence and security agencies.

The aim of this book is to examine the many challenges of implementing effective democratic and parliamentary oversight of the intelligence sector. In this concluding chapter, attention is first given to lessons learned from the analyses presented in this volume. This chapter will be structured according to the major themes of the four parts of the book: reform of intelligence in Eastern Europe; intelligence reform in the West; the role of parliaments in the oversight of intelligence services; and finally, data protection and the public's right of access to information. The second part of the concluding chapter will be devoted to proposals for strengthening the democratic control of intelligence services by enacting comprehensive frameworks; putting safeguards in place against

politicisation of the intelligence services; internal oversight mechanisms within the services; assuring loyalty of intelligence employees in transition states; and, strengthening the role played by parliament and the public.

## Taking Stock of the 'Democratic Control of Intelligence Services'

### *Reforms in Eastern Europe*

Intelligence services in the Eastern European countries treated in this volume have been the products of their respective environments. As the tools of centralised power under authoritarian rule, they were characterised by opaque cultures of cronyism, corruption and repression with impunity. After the fall of communism, the mode of transition to democracy conditioned the future shape of the intelligence services; in Poland where the transition was discussed and negotiated over time, the services had time to prepare for a new role in a new setting thus securing their interests in the new arrangements and perpetuating informal power networks. In the cases of Czechoslovakia (in Chapter 6 the focus was on the Czech Republic as one of the two successor states) and Romania on the other hand, sudden and hasty transitions, which changed the role of the services overnight, would become a factor in the ensuing disorder characteristic of their reorganisation. The degree of violence and repression in which the Romanian services were engaged, affected future attitudes towards reform and the role of democratic oversight; so great was the deficit of public trust that intelligence activity was strongly curtailed in the first 18 months of the transition period. In Czechoslovakia, the suddenness of the transition resulted in the anomalous situation of the communist era intelligence services systematically destroying all trace of their activities while the country's first democratically elected government went about the business of transition.

During the 1990s, when reform became the order of the day, the importance of democratic intelligence oversight was sometimes overshadowed by economic issues (as in the Czech Republic under Václav Klaus); or conversely, became the first order of business in societies traumatised by their experience of the abuse of power (as in Romania). The early years of this decade of reform, until the mid-1990s, were characterised by efforts to dismantle the communist structures, including substantial reductions in personnel numbers (as in Poland, Romania and Czechoslovakia) and extensive restructuring of the intelligence services. In some cases the effectiveness of these reforms was jeopardised by former regime elements who retained influence and were able to co-opt the process (as in Poland and Bulgaria). Also the severe lack of suitably qualified personnel made the new intelligence services dependent on the cadres of the former regimes (as in Czechoslovakia and Romania). From the mid-1990s on, reform efforts were bolstered with the introduction of better oversight structures and more

thorough vetting procedures and lustration processes (see Poland's lustration law 1997; Bulgaria's restructuring in 1997; 1994 legislation in the Czech Republic; and, Romania's constant reduction of ex-*Securitate* personnel).

However, after a long decade of variously successful moves towards accountability and transparency, a kind of transition fatigue has become visible in all cases. The political will to carry difficult reforms to their conclusion has sometimes been found wanting (as in Bulgaria), or the implementation of oversight mechanisms once in place has been uneven (as in Romania). At the extreme end of the scale, intelligence services have become a vehicle for the capture of influence by elites and thereby have been deeply implicated in informal power networks (as in Poland). Similarly, democratic oversight has not been able to prevent intelligence services from trading their political neutrality for political influence (as in the case of the Romanian SRI under the direction of Magureanu who used his post to jockey for political position). This underlines the fact that the delicate balance has not yet been struck between the usefulness of skilled personnel from another era and the imperatives of democratic oversight in modern intelligence services.

The balance has also been skewed between intelligence gathering and the need for disclosure and respect of human rights: excessive secrecy paralysed processes of reconciliation with the past in Hungary, while in Romania civil unrest was allowed to become a dangerous threat to national security because intelligence gathering was so disrupted for a time. Nevertheless, closer interaction with outside agencies and increasingly close working relationships with bodies such as NATO and the European Union have been key drivers in the push for further reform but not necessarily towards better democratic oversight. On the contrary, various Eastern European states, for example Bulgaria, have adopted stricter access to classified information laws, under the threat of rejection of NATO membership. This trend of stricter access to classified information has been exacerbated by the events of 9/11, which have created an atmosphere of increased secrecy, and for the moment stifled the momentum for further reforms (as in the Czech Republic, Hungary and Bulgaria where the Classified Information Act of 2002 has been used to legitimate the lack of further reform).

*Reforms in the West*

The drive towards better democratic oversight of intelligence services in the West traces its origins to the demands of citizens to have their rights respected by the governments who act in their name. The flagrant misuse of intelligence services to monitor the legitimate activities of private citizens sparked scandal and controversy in the United States, Norway and France. Responses to public pressure for increased accountability have varied from a comprehensive overhaul of the entire system (as in the United States in the 1960s and 1970s), to truncated enquiries whose results are not disclosed (as in France). In Norway, scandal had to await the

fundamental change in perceived threats to national security which came with the end of the Cold War, in order for the political conditions conducive to increased democratic oversight to emerge.

The momentum behind these moves towards more transparency and accountability has resulted in a range of responses from passive to pro-active systems of democratic oversight, including parliamentary intelligence oversight committees with a mandate to oversee compliance of the services with human rights regulations and the rule of law (as in Norway), or finance, policy and administration of the services (as in the UK), or further, all aspects of the functioning of intelligence services, including operational activities (as in the US). France on the other hand, stands alone among Western countries in rejecting the fundamental concept of democratic oversight and manages its extensive intelligence gathering network exclusively through executive control. Pressure from the public for effective democratic governance has helped encourage oversight bodies to become catalysts in reform processes and policy reformation (as in the United States and Norway). In the United Kingdom, reform of oversight procedures was driven by outside pressures to conform to democratic norms, in particular as set down by the European Convention of Human Rights (ECHR) and case law of the European Court of Human Rights (ECtHR). Furthermore, for other (domestic) reasons, France is also currently studying the feasibility of a special parliamentary intelligence oversight committee.

The aftermath of 9/11 has increased the importance of quality intelligence in all the countries concerned, tilting the balance away from respect of human rights towards increasingly intrusive intelligence gathering measures. This recalibration has reverberated differently in each system, such that in France, for example, it has meant affording fewer rights to suspects and subjects of surveillance, while in Norway intelligence services have argued for the need to interpret central protective provisions of the law in a limited way. This reorientation of values reproduces itself subtly in each system and reflects the same shifts that have been observed in Eastern Europe.

*Parliamentarians*

Parliamentary oversight is the necessary counterweight to executive control in a liberal democracy and its responsibilities should include ensuring transparent budget oversight, the legality of the services and their efficacy. On the condition that such oversight functions within a broader governmental framework of transparency and openness, critical oversight can augment public faith in the services. The risk also exists that services can be drawn into political wrangling, that information could become sensationalised or that parliamentarians will simply be uninspired by a relatively thankless task. Often intelligence oversight is a thankless task for parliamentarians because intelligence reforms usually do not attract large numbers of voters; this is exacerbated by the fact that classified

information cannot be communicated to the public. A political culture of transparency and the appreciation on the part of politicians of the importance of oversight are hence key factors in ensuring its success.

Across most mature and new democracies parliamentary oversight committees have been created only in the last three decades since the mid 1970s. Their mandates vary from reactive to proactive and can be broad (as in the United States or Canada), or narrow (as in Norway, Poland or the United Kingdom). Committees are either composed of parliamentarians (as in the United Kingdom) or approved external experts (as in Norway) but the degree of parliamentary ownership over the oversight process itself is the more crucial factor in determining their ability to ensure accountability and transparency. They are usually vested with investigatory powers but can be hampered by imperfect access to classified information, lack of resources and expertise.

In the example of the United Kingdom, the public mistrust built up over long years of official denial of its intelligence services was helpfully assuaged by the establishment of the Intelligence and Security Committee. Since its inception its powers have been weak (but well used in practice) and it has run the risk of becoming politicised through the controversy surrounding the intelligence on WMD in Iraq supplied to the government in the lead up to the war. A more permissive attitude towards the use of outside sources and disclosure of information could help correct the perception of an oversight body too close to the centre of power.

The post-9/11 trend has tended away from increased disclosure and better protection for human rights towards increased intelligence gathering capabilities and more effective services in the wake of what was seen as a colossal failure in intelligence gathering. For parliamentary oversight this has meant struggles over access to information in a context of increased secrecy, and an increased need for intelligence services to be seen as effective creating pressure on oversight bodies to tolerate misbehaviour. Legal assertions of power have extended the remit of intelligence services to conduct surveillance and gather information but this trend threatens to jeopardise hard-learned lessons of past decades about the value of robust democratic oversight and the need to place limitations on intelligence services. These trends can be counterbalanced by promoting coordination and the exchange of ideas and best practices within the ‘oversight community’ across states as well as by promoting an even greater vigilance on the part of those serving on oversight bodies and the public at large.

*Data Protection and Access to Information*

An increasing number of countries have chosen to enact Freedom of Information legislation (FOI laws) but the degree of access to information that these mechanisms afford varies and often excludes important categories. Backed up by pressure from international organisations (for example the World Bank) and public pressure at home, (international) norms of good governance, have been key in the

drive toward increased transparency. Transitions to democracy and assertions of constitutional rights as well as the role of regional organisations such as the European Court of Human Rights have also been factors. Crises and scandals have also added momentum to anticorruption campaigns demanding better oversight and access to classified information

Most FOI laws are similar in that they protect the individual's right to government information without further legal grounds. They create a duty on government to inform and to publish information and they also define exceptions. The specific definition of what counts as information to be disclosed is thus crucial in establishing the reach of such legislation and has created serious gaps in credibility and usefulness. The disclosure of information is also often made subject to harm and public interest tests as a way of striking a balance between national security and public interest. All decisions are subject to review and the court is the final arbiter. Some laws provide for internal review processes (Australia) but most also have external procedures of which the ombudsman is the most common. Information commissioners are also a feature in certain systems (the United Kingdom and Hungary for example).

Schemas of classification of information are set down in State Secret Acts and define the parameters of oversight as well as limitations on and the duration of classification. In Eastern Europe, as mentioned earlier in the case of Bulgaria, the passing of state secrets legislation to meet the requirements of NATO adhesion has disrupted many new democracies in their development of cultures of openness and state accountability (see Chapter 13 on FOI laws). Some Eastern European nations had adopted special laws to govern access to communist era information such as former secret police files (Romania and Czechoslovakia); others used lustration committees to accomplish the same goals of reconciliation with the past (Hungary).

Some of the problems posed by excessive secrecy include the potential for political manipulation of access, the non-disclosure of embarrassing information, and the covering up of abuses and corruption. Furthermore excessive secrecy imposes significant monetary costs involved as well as adversely affecting the sharing of information among intelligence services with associated losses in efficacy.

In the Hungarian case, the recommendations of the Data Protection Commissioner are non-binding, and although the powers of the office are relatively broad, including a right to inspect premises and supervise classification procedures, they do not provide for the conduct of investigations. Despite these limited powers, the Data Protection Commissioner has been able to exert a significant degree of oversight discovering various violations on the part of the intelligence services and bringing these to the attention of the public. Informational rights were protected through the Office of Hungarian Data Protection Commissioner in cases concerning the abuse of classification rules regarding Russian debt payments (1996), the improper disclosure of cabinet proceedings (1998), and the illegal surveillance of civilians (1990–1995). In each case, the high degree of respect for the Office of the Commissioner and the

ensuing publicity of its findings put pressure on the executive to accept the Commissioner's recommendations.

Data protection and access to information are both part of so-called informational rights. These rights play a pivotal role in the effective oversight of intelligence services as they require that government make information available to the public. Even if this information becomes available after only 10–20 years, it still plays an important role in holding intelligence services accountable *ex post factum*. In this context, 9/11 has had a negative effect on the accountability of intelligence services, as various countries, notably the US, have adopted a more expansive view of national security to the detriment of the public's right of access to government information.

## Strengthening Democratic Control of Intelligence Services

Various authors in this volume have asserted that democratic control of intelligence services should be perceived as a multi-level system of governance. This implies firstly that democratic control does not depend on elected politicians in parliament only, but also depends on the effectiveness of other oversight mechanisms at the level of the intelligence agencies themselves, the executive, parliament, courts and the general public and even international organisations who set standards for intelligence oversight (for example the Council of Europe and its ECHR). Multi-level security sector governance can be seen as a framework of oversight consisting of (a) state and civil society actors, both on the domestic and international level (b) based on norms of legality, efficiency, transparency and accountability in order to (c) check whether the services comply with these norms. The following discussion focuses on recommendations for strengthening the governance of intelligence services.

### *Enacting a Comprehensive Legal Framework*

Nearly all chapters referred to the need for enacting an up-to-date and comprehensive legal framework for the accountability and functioning of intelligence services. The significance of laws goes beyond their legal impact: laws enacted by parliament are also the embodiment of the democratic will of the people.

The analyses in this volume show that transition to democracy (the Czech Republic, Romania and Bulgaria), scandals (Norway and the US) or legal challenges (the UK) are triggers for enacting or amending legal frameworks. It is not self-evident that democracies have intelligence services based on a statutory law enacted by parliament. For example, intelligence services were legally invisible in the UK until 1989. In France, intelligence services are all based on governmental decrees instead of laws enacted by parliament, signifying that parliament is sidelined in formulating the legal parameters of intelligence services. The answer to the question 'What are the elements of a comprehensive legal framework?' could easily justify an entire book. Without pretending to be

complete, the following could be mentioned.

One important element of any legal framework of intelligence services is the protection of human rights, in particular with regard to the special powers of intelligence services to interfere with private communication and property (for example surveillance operations, house searches etc.). An interesting approach for protecting human rights can be found in the ECHR. Although the ECHR permits restrictions on human rights if necessary in a democratic society for the protection of national security (for instance the right to privacy), it demands that any restriction be authorised by law. From this approach it can be learned that proportionality and authorisation by law are essential elements of a legal framework. Another important element of the legislation is to define the mandate of the intelligence services by law. This is a safeguard against changes in the intelligence services' mandate without parliamentary authorisation. Related to the mandate and functioning of the services, intelligence laws need to cover the geographical area of operations, the scope of threats to national security, the protection of human rights authorisation mechanisms for the use of special powers, relations between the services, executive and parliament as well as the status of intelligence employees and the use of public funds.

*Safeguards against the Politicisation of Intelligence Services*

Various chapters in this volume demonstrate the need for strong executive oversight of intelligence services. For example, Chapter 6 on the Czech intelligence services shows that strong political executive leadership was needed in order to abolish the old communist services and to set up new services after the 1989 'Velvet' revolution. However, other analyses presented in this volume suggest that strong executive leadership should not amount to political misuse and politicisation of the services. From Chapter 12 on post-9/11 intelligence oversight by Peter Gill, we learn that politicisation is caused by a relationship that is too close between the political leadership and the intelligence services, when political leadership has the power to alter (the presentation of) intelligence in such a way that it suits policy decisions which have already been made. From the Rainbow Warrior scandal, described in Chapter 8 on the French intelligence services, it can be learned that political leaders apply the strategy of 'plausible deniability' to refute any involvement in illegal covert operations (in this case the blowing up of a Greenpeace ship which caused the death of one crew member). The French structures for governing intelligence services allowed for plausible deniability because of the predominant position of the executive *vis-à-vis* a parliament with weak intelligence oversight powers.

From these instances of political misuse of intelligence services it can be learnt that intelligence collection, analysis and reporting should be strictly isolated from political decision-making. Secondly, it demonstrates the need for all directives from the political leadership to the intelligence services to be put down

in writing with a copy supplied to an independent audit body (appointed by the executive), for example an inspector-general (see below).[1] In this way political leaders cannot avoid accountability for their decisions. Both cases also show that strong parliamentary oversight over the executive is another important element for avoiding political misuse of the services by the executive.

*Internal Oversight within the Intelligence Services*

Another important issue is to check whether laws and policies are correctly implemented by the intelligence services. As was mentioned in Chapter 12 on post-9/11 intelligence oversight, in search of better democratic control, improved legal rules alone will be insufficient as it is necessary to deal with the reality and culture of intelligence agencies as well. Indeed, there is the danger that once legal reform is achieved, it will be assumed that 'real change in the agencies and their behaviour will result' (Chapter 12). Indeed, cultural change within the agencies has to be considered as a long term project, in particular for those agencies which were out of control and which were acting as 'rogue elephants'. In this context, it is relevant to take internal oversight within the agency into account. Internal oversight is a safeguard that illegal activities or human rights violations do not start in the first place. In this volume the issue of internal oversight is referred to in the context of inspector generals for intelligence services as well as internal oversight offices. Inspector generals for intelligence services exist, for example, in the US, Canada, Australia and Bosnia-Herzegovina. Typically, the role of the inspector general is to review the operational activities of the agencies with a focus on legality, propriety and human rights (as is the case, for example, in Australia). They are often able to conduct independent inspections and inquiries. Another example of internal oversight is given by Chapter 7 (intelligence oversight within the US Department for Defense). The Office of the Assistant to the Secretary of Defense for Intelligence Oversight is charged with independent oversight of all intelligence, counterintelligence and intelligence related activities in the Department of Defense. This Office focuses not only on *ex post factum* oversight, but is also dealing with awareness, education and training as well as giving tailor-made policy advice. In particular, training of intelligence offices in relevant legislation and policy is used as a way to prevent the occurrence of breaches of the law. However, recent scandals such as the Abu Ghraib scandal (brutalising of prisoners by US forces, including military intelligence) as well as the alleged involvement of the US intelligence services in the illegal detention and transportation of terrorist suspects, illustrate that internal oversight is not sufficient for at least two reasons. Firstly, as the Abu Ghraib scandal illustrates, private intelligence companies were involved in

1. For further information on avoiding political abuse of intelligence services, see Hans Born and Ian Leigh, 2005, pp. 68–71.

the interrogation (amounting to abuse) of prisoners. Private intelligence services normally do not fall within the remit of internal oversight and other accountability mechanisms need to be developed to ensure that private intelligence services are held accountable. Secondly, these recent intelligence scandals demonstrate the need for an executive leadership that adheres to international humanitarian law as a framework of action for intelligence operatives.

*Assuring the Loyalty of Intelligence Employees in Transition Countries*

Particularly in post-authoritarian states, the issue of loyalty among intelligence employees is problematic. To what extent are intelligence officials who worked in the old authoritarian structures (for example the *Securitate* in Romania) loyal to the new democratic structures? In addressing this question, two basic models can be distinguished. A first option is that, for the sake of efficacy, the successor service relies substantially on the officers of the former (often repressive) intelligence service. This model was followed by the Romanian domestic intelligence service (SRI). The former *Securitate* officers formed 60 percent of the new SRI in 1990, although this rate had dropped to 20 percent by 2002 (see Chapter 3 on reform of the Romanian intelligence services). A second option is to make a radical break with the past and not to hire any former employees into the new intelligence service. This model was followed by the foreign intelligence service in the Czech Republic, where the old operatives were replaced by new recruits. This decision had a positive impact on the willingness of western intelligence services to cooperate with the new structures as well as being an assurance 'against old communist skeletons coming out of the closet at a time when the country least needed it' (Chapter 6). However, former dissidents are not necessarily good spies or counter-spies. In this context, the new intelligence services in the Czech Republic greatly benefited from the support of their Western counterparts.

*Strengthening the Role of Parliament*

The need for strong parliamentary oversight of intelligence services was covered by all chapters in this volume. Parliamentary oversight can be seen as a safeguard against executive misuse of intelligence services (see above), a form of public accountability which can contribute to public trust in the services, and an added assurance of the efficient use of taxpayer's money. Strong parliamentary oversight consists of three elements which can be referred to as the 'triple A of parliamentary oversight'. Firstly, 'Authority' which refers to the statutory powers of parliament, including the power to control the (entire) intelligence budget, to conduct hearings and inquires, to subpoena members of the government, to enact or amend intelligence laws, monitoring the management, policy and administration of intelligence services as well as (for example in the US) monitoring and prior authorisation of special operations. Secondly 'Ability', referring to information,

expertise and resources to back up the oversight mandate of parliament. Lastly, 'Attitude', which refers to willingness on the part of parliamentarians, especially the members of the parliamentary intelligence oversight committee, to take an active approach to intelligence oversight including raising critical questions with Cabinet Ministers, initiating investigations into questionable conduct of intelligence services, and requesting sensitive (classified) information if need be. At the core of parliamentary oversight stands a specialised parliamentary intelligence oversight committee, which can operate independently from the executive in terms of appointing the chair and members of the committee, deciding on a work programme, appointing staff as well as reporting to parliament and the public. Chapter 11 on the UK shows that the relatively new Intelligence Security Committee (ISC) of the UK parliament does not meet these criteria as the prime minister appoints the chair and members of the ISC as well as censors the reports of ISC. Nevertheless, in spite of these and other limitations, Ian Leigh concludes that the ISC 'has worked well despite its relatively weak powers' (see Chapter 11).

Another interesting idea for strengthening parliamentary oversight is based on Gill's analysis of post-9/11 intelligence oversight. The claim can be made that increasing international cooperation between services should be matched by increasing international cooperation between intelligence oversight bodies. It is only in recent times that internal review bodies[2] and that parliamentary intelligence oversight committees of EU member states[3] have met on a regular basis. Additionally, foundations like DCAF bring together parliamentarians and their staff for the purpose of information exchange and training. However, no matter how informative these gatherings are, they cannot equal international bodies in the oversight of international intelligence cooperation.

2. The International Intelligence Review Agencies Conference (IIRAC) meets on a bi-annual basis. For example, in October 2006 the IIRAC met in South Africa and its participants included representatives of intelligence review bodies of Australia, Belgium, Canada, the Netherlands, New Zealand, Norway, Poland, South Africa, the United Kingdom as well as the United States of America and representatives of Ghana, Namibia and Tanzania. See: http://www.info.gov.za/speeches/2006/06110211151004.htm.
3. The parliamentary intelligence committees of EU member and candidate member states as well as observers of various other countries meet on a regular basis, most recently Bucharest in October 2006.

*The Role of the Public*

Various chapters underline the fact that intelligence agencies need to enjoy public trust in order to function effectively. A lack of public trust can be measured by critical and negative media reports about the services, leading members of parliament to take a critical stance toward the services, and complaints from citizens and NGOs about the working methods of the services. A negative public attitude toward intelligence services does not arise automatically but is often based on the history or current conduct of the intelligence services. In particular in transition societies where intelligence services were previously used for protecting the ruling elite against their own people, the public has a negative predisposition towards intelligence services. Alternately, one cannot expect public trust if the services were not able to avert security threats or were involved in illegal activities, including unlawful intervention in public and political life (for example selectively releasing files of politicians and journalists as happened in Romania, Bulgaria and Poland). Increasing public accountability is one of the major ways to increase public trust, for example by submission of the services to parliamentary accountability, annual public reports about the functioning of the services as well as the establishment of the services' mandate and special powers by (publicly available) law.

Data protection and freedom of information laws are also important tools for enabling public scrutiny. In particular accountability can be enhanced if the media and public at large have the possibility to demand access to classified information after a certain period of time.

## Conclusion: Who guards the guards?

In this volume numerous challenges to intelligence oversight are addressed, such as the need for transparency versus the legitimate need for secrecy; the need for balanced and mature oversight by parliamentarians who are not intelligence professionals themselves; the need to keep intelligence services isolated but not insulated from the political fray; regarding intelligence legislation as the starting point but not the end point for improving democratic accountability; and, the need for both passive and proactive oversight. The contributors to this volume all echo the wider conviction that oversight of intelligence services is an indispensable element of democracy for ensuring the services' legality, propriety, efficiency and respect of human rights. In particular in the post-9/11 context, it is important that the powers exercised by intelligence services are limited and proportionate to the threats. In answering the question of who is guarding the guards, it is a hopeful sign that public accountability of intelligence services has become an internationally established practice in nearly all liberal democracies around the world.

Nevertheless, there is a need for a future agenda to improve both intelligence accountability and academic research on the reform and oversight of intelligence services. Based on the studies in this volume, it can be concluded that the most pressing issues are the oversight of international intelligence cooperation; the accountability of private intelligence companies; culture and professional commitment of intelligence services towards democratic accountability, rule of law and human rights; and, the further development of reform models for intelligence services.

*This page intentionally left blank*

# Bibliography


Achim, S. (2001), 'In Presa si Biserica Ortodoxa se gaseau si urmariti, si turnatori la Securitate' [In the Press and the Orthodox Church one finds those followed and those who betrayed them to the Securitate], *Adevarul*, 6 October, Romania.

Adler, A.R. (1992), *Litigation under the Federal Open Government Laws*, ACLU, New York.

Allen, M. and Eilperin, J. (2002), 'Cheney Blames Leaks on Congress', *Washington Post*, 21 June.

Allen, M. and Mintz, J. (2002), 'Homeland Department May Take a Year to Take Shape', *Washington Post*, 21 November.

Al-Wahab (1983), *The Swedish Institution of Ombudsman*, Greenwood Press, London.

AMC (1996), 'Minister oskarża "Wprost"' [The minister accuses 'Wprost' {title of a Polish weekly}], *Życie,* Poland, 7–8 December, edition B, p. 5.

Andrew, C. (1987), *Secret Service: The Making of the British Intelligence Community*, Viking Press, Sevenoaks.

Andrew, C. (1991), 'The British View of Security and Intelligence', in A.S. Farson, D. Stafford and W. Wark (eds), *Security and Intelligence in a Changing World*, Frank Cass, London, pp. 10–24.

ANT (2001), 'Oficer fałszerz' [Officer forger], *Gazeta Wyborcza, Gazeta w Bydgoszczy*, Poland, 2–3 June, p. 3.

Armstrong, S. (1998), 'The War over Secrecy: Democracy's Most Important Low-Intensity Conflict', in A.G. Theoharis, (ed.), *A Culture of Secrecy: The Government Versus the People's Right to Know*, University Press of Kansas, Kansas, pp. 140–186.

Assassination Records Review Board (1998), *Final Report of the Kennedy Assassination Records Review Board*, September, available at: http://www.fas.org/sgp/advisory/arrb98/.

Assembly of the Western European Union (2002a), *The New Challenges Facing European Intelligence – Reply to the Annual Report of the Council*, Document A/1775, 4 June, available at: http://www.assembly-eu.org/en/documents/sessions_ordinaires/rpt/2002/1775.html.

Assembly of the Western European Union, (2002b), *Parliamentary oversight of the intelligence services in the WEU countries – current situation and prospects for reform*, Document A/1801, 4 December, pp. 5.

*Associated Press* (2004), 'Anti-Terrorist Unit Used for Political and Personal Vendettas', 16 November.

AZ, DM, BEL (1999), 'Tygrys z Arizony', *Gazeta Wyborcza*, Poland, 10 September, edition BYT, p. 2.

Baer, R. (2002), *See No Evil*, Crown Publishers, New York.

Bailey, S., Harris, D. and Jones, B. (2002), *Cases and Materials on Civil Liberties*, 5th edn, Butterworths, London.

Baleanu, V.G. (1995), *The Enemy Within: The Romanian Intelligence Services in Transition*, Conflict Studies Research Centre, Camberly, January.

Baleanu, V.G. (1996), *A Clear and Present Danger to Democracy: The New Romanian Security Services Are Still Watching,* Conflict Studies Research Centre, Camberley.

Bamford J. (2005), *A Pretext for War: 9/11, Iraq, and the Abuse of America's Intelligence Agencies*, Anchor Books, New York.

Banisar, D. (2004), *Freedom of Information and Access to Government Record Laws Around the World*, available at: http://www.freedominfo.org/survey.htm.

Banisar, D. (2006), *Freedom of Information around the World 2006: a Global Survey of Access to Government Information Laws*, Privacy International, London. Available at: http://www.privacyinternational.org/foi/foisurvey2006.pdf.

Barański, M. (1997), 'Przepraszamy Kaczyńskiego' [We apologize Kaczyński], *Nie*, Poland, 21 August, p. 1.

Barański, M. (1998), 'Służbówka posła Miodowicza' [A half official apartment of Mr. Miodowicz, the MP], *Nie*, Poland, 22 January, p. 1.

Barański, M. (2001), *Bunt janczarów: Kulisy tajnych służb Trzeciej Rzeczypospolitej* [A revolt of servants: Secrets of the intelligence services of Post-Communist Poland], Warszawa, Poland, PPUH 'ALMAR'.

Basiewicz, M. and Snarski, P. (2003), 'Lobbyści – czwarta władza' [Lobbyists – the fourth power], *Przegląd*, Poland, 13 April, pp. 12–16.

BBC Monitoring Service (1990), Summary of World Broadcasts, EE/0932, 27 November, p. B/10.

BBC News (2004a), 'Ex-KGB man backs new MI6 Chief', 7 May, available at: http://news.bbc.co.uk/2/hi/uk_news/politics/3689779.stm.

BBC News (2004b), 'No Regrets for Sacked Spy Expert', 29 October, available at: http://news.bbc.co.uk/1/hi/uk_politics/3965775.stm.

BBC News (2004c), 'GCHQ Translator Cleared over Leak', 26 February, available at: http://news.bbc.co.uk/1/hi/uk/3485072.stm.

Belciuganu, R. (2001), 'Timofte ordona o ancheta totala in SRI' [Timofte orders a total investigation in the SRI], *Jurnalul National*, 16 May, Romania.

Belu, M. (2001), 'Generalul Mihai Caraman, fost sef al SIE pana in 1992, confirma: "Voiculescu a fost unul dintre cei mai importanti clienti ai firmei Securitatii, ICE Dunarea"' [General Mihai Caraman, former chief of the SIE up until 1992, confirms: 'Voiculescu was one of the most important clients of the Securitate firm ICE Dunarea'], *Cotidianul*, 26 June, Romania.

Berdeli, E. (2001), 'Stafia rosie din conacul SRI' [The red spectre in the SRI house], *Cotidianul*, 11 May, Romania.

Berkowitz, B. and Goodman, A. (2000), *Best Truth: Intelligence in the Information Age*, Yale University Press, New Haven and London.

Biernacki, M. (2002), *Polska bez mafii ….* [Poland without mafia...], Interviewed by M. Trzciński. Wydawnictwo MOST, Warsaw, Poland.

Bigo, D. (1994), 'The European Internal Security Field: Stakes and Rivalries in a Newly Developing Area of Police Intervention', in M. Anderson, and M. den Boer (eds), *Policing Across National Boundaries*, Pinter Publishers, London.

Blanton, T. (2003), 'National Security and Open Government in the United States, Beyond the Balancing Test,' in *National Security and Open Government: Striking the Right Balance*, Campbell Public Affairs Institute, Syracuse University.

Borger, J. (2002), 'For Their Eyes Only', *The Guardian*, 6 March.

Born, H. (2004), 'Towards Effective Democratic Oversight of Intelligence Services: Lessons Learned from Comparing National Practice', *Connections-Quarterly Journal*, Vol. III, December, pp. 1–12.

Born, H. and Leigh I. (2005), *Making Intelligence Accountable: Legal Standards and Best Practice for Oversight of Intelligence Agencies*, Publishing House of the Parliament of Norway, Oslo.

Born, H., Johnson, L. and Leigh, I. (eds) (2005), *Who's Watching the Spies? Establishing Intelligence Service Accountability*, Potomac Books Inc., Dulles, VA.

Brown, J. F. (1994), *Hopes and Shadows: Eastern Europe after Communism*, Duke University Press, Durham.

Bucura, D. (2001a), 'Radu Timofte – victima a Securitatii' [Radu Timofte – a victim of the Securitate], *Adevarul*, 26 April, Romania.

Bucura, D. (2001b), 'Scandalul 'Timofte – agent KGB' a fost declansat din interiorul SRI [The 'Timofte – KGB agent' scandal was launched from within the SRI], *Adevarul*, 7 May, Romania.

Bureau of National Security (1996), *Recommendation of the Data Protection Commissioner Summarizing the Investigation of National Security Checks Performed Since 1990*, Bureau of National Security, Budapest (7/A/1995).

Butkiewicz, T. (2003), 'Dymisja za poręczenie' [Dismissal for a pledge], *Życie Warszawy*, 20 March, Poland.

Butler (2004), *Review of Intelligence on Weapons of Mass Destruction*, Report of a Committee of Privy Counsellors HC898, The Stationery Office, London, July 14.

Cameron, I. (2000), *National Security and the European Convention of Human Rights,* Kluwer Law International, Dordrecht.

Cameron, I. (2005), 'Beyond the Nations State: The Influence of the European Court of Human Rights on Intelligence Accountability', in Born, Johnson and Leigh (eds) *Who's Watching the Spies? Establishing Intelligence Service Accountability*, Potomac Books Inc., Dulles, VA.

Caparini, M. (2002), 'Challenges of Control and Oversight of Intelligence Services in a Liberal Democracy', *Workshop on Democratic and Parliamentary Oversight of Intelligence Services*, Geneva Centre for the Democratic Control of Armed Forces (DCAF), Geneva, 3–5 October.

Carothers, T. (1996), *Assessing Democracy Assistance: The Case of Romania*. Carnegie Endowment for International Peace, Washington.

CBOS (2002), 'Jacy jesteśmy? Zaufanie Polaków do ludzi i instytucji publicznych oraz gotowość do współpracy' [What are we? Trust in public figures and institutions and willingness to co-operate], Public opinion poll report, Poland, available at: http://www.cbos.com.

C.D. (2002), 'SRI intra in topul increderii romaniilor. Biserica ramane pe primul loc' [The SRI enters into the top of most trusted by Romanians. The Church remains in first place], *Azi*, Romania, 30 September.

Celiński, A. (2003), Interviewed by M. Barański, *Trybuna.* 26 April, cited in *Gazeta Wyborcza*, Poland, 28 April, p. 2.

Cenckiewicz, S. (2003), 'Służba bezpieczeństwa wobec I Krajowego Zjazdu Delegatów NSZZ "Solidarność"' [Communist Security Service operations against the First National Congress of Solidarity Trade Union], *Arcana*, Vol. 51-52 (3–4), Poland, pp. 94–125.

Center for International Policy (1996), *The Failure of Intelligence Review: A critique of three recent commission reports exonerating the CIA*, available at: http://www.us.net/cip.proceed.htm.

Cepik, A. and Antunes, P. (2001), *The New Brazilian Intelligence Law: an Institutional Assessment*, Paper given to the Centre for Hemispheric Defense Studies, Washington DC.

Chapman, B. (1970), *Police State*, Pall Mall, London.

Childs, D. and Popplewell, R. (1996), *The Stasi. The East German Intelligence AND Security Service*, NYU Press, New York.

Cieśla, W. (2003), 'Na kłopoty – FOZZ' [In case of troubles – FOZZ], *Gazeta Wyborcza*, 17-18 May, pp. 18–19, Poland.

Cieśla, W. and Jachowicz, J. (2002), 'Big Brothers, czyli wojna agentów' [Big Brothers, or war of secret agents], *Gazeta Wyborcza*, 2-3 November, Poland, pp. 12–15.

Commission nationale de l'informatique et des libertés (CNIL) (2004), *Réforme de la loi de 1978*: *principaux amendements adoptés par l'Assemblée Nationale* [Reform of the 1978 Law: principal amendments adopted by the National Assembly], Section 'Le contrôle des services secrets', available at: www.cnil.fr/index.php?id=1575&print=1.

Constantin, C. R. (2002), *Serviciile Secrete din Romania si Scandalurile de Coruptie: 1989–2001* [Romanian Secret Services and Corruption Scandals: 1989-2001], Antet XX, Bucharest, Romania.

Cotidianul (2001), [article noting vetting of parliamentarians and that 8 ANP candidates ex-Securitate affiliations], 25 April, Romania.

Cotidianul (2002), 'Securitatea, puterea invizibila' [The Securitate, the invisible power], *Cotidianul*, 12 July, Romania.

Council of Europe – Venice Commission (1998), *Internal Security Services in Europe*, Council of Europe, Strasbourg (CDL-INF [1998] 6e).

Council of Europe Committee of Ministers, *Declaration on the Freedom of Expression and Information*, 29 April 1982. Clause 8. II. C.

Cychol, D. (2001), 'Z czego żyją szpiedzy' [How spies make earnings], *Nie*, Poland, 2 August, p. 1.

Cychol, D. (2003), 'Prawda, z którą mija się Tober' [Truth avoided by Tober], *Nie*, Poland, 17 April, p. 3.

Czajkowska (1999), 'Tajemnica raportu UOP' [A secret on account of the Office of State Protection], *Gazeta Wyborcza*, Poland, 25 May, p. 1.

Danchev, A. (2004), 'The Reckoning: Official Inquiries and the Iraq War', *Intelligence and National Security* 19:3, pp. 436–466.

Darski, J. (1992), *Tajni współpracownicy policji politycznej w państwach postkomunistycznych* [Secret collaborators of the political police in Post-Communist States], Instytut Polityczny, Warsaw, Poland.

Daun, A. (2005), 'Intelligence – Strukturen für die mulitlaterale Kooperation europäischer Staaten', *Integration*, [Intelligence - Structures for multilateral cooperation of European countries], Vol. 28, April, pp. 135–149.

Davies, P. (2004), 'Intelligence Culture and Intelligence Failure in Britain and the United States' *Cambridge Review of International Affairs*, Vol. 17, No. 3.

DCAF Intelligence Working Group (2003), *Intelligence Practice and Democratic Oversight – A Practitioner's View*, Occasional Paper, No. 3, Geneva Centre for the Democratic Control of Armed Forces, July.

Decree of the Council of Ministers 26/1990 III.14, Hungary.

Deletant, D. (2001), 'The Successors to the Securitate: Old Habits Die Hard' in K. Williams and D. Deletant, *Security Intelligence Services in New Democracies: The Czech Republic, Slovakia and Romania*, Palgrave, London, pp. 211–262.

Deletant, D. and Williams, K. (2001), *Security Intelligence Services in New Democracies: The Czech Republic, Slovakia and Romania*, Palgrave, London.

Department of Justice (2002), *Fact Sheet: Attorney General's Guidelines for Information Sharing*, 23 September. Available at: www.usdoj.gov.

D.Fr. (2002), 'Czystka pod pretekstem reformy' [A purge under the pretext of reform], *Rzeczpospolita*, 23 October, Poland.

DIA (1997), *The Genesis of Intelligence Oversight*, DIA Joint Military Intelligence Training Centre.

Diac, M. (2001), 'Cazul 'Timofte – KGB este inchis, dar in interiorul SRI au mai fost 'fabricate' si alte dosare' [The 'Timofte – KGB case is closed, but other files were also 'fabricated' within the SRI], *Adevarul*, 10 May, Romania.

Diamond, L., Plattner, M.F. and Schedler, A. (eds), (1999), '*The Self-Restraining State: Power and Accountability in New Democracies*, Lynne Rienner Publishers, Inc., London.

Dimitrov, E. (2002), Commission on State Security Records, *SEGA* newspaper, 5 September, p. 7.

Dobran, V. (2002), 'SRI a interceptat convorbirile lui Pavalache' [The SRI intercepted Pavalache's conversations], *Cotidianul*, 30 October, Romania.

Dudek, A. (2004), *Reglamentowana rewolucja. Proces rozkładu komunistycznej dyktatury w Polsce (1988–90)* [A Controlled Revolution: The Process of Decline of the Communist Dictatorship in Poland], Arcana, Kraków, Poland.

Dukaczewski, M. (2001), Interviewed by A. Walentek, *Życie Warszaw*, 4 December, Poland.

Dyson, J. (1986), *Sink the Rainbow Warrior! An Enquiry into the Greenpeace Affair*, London, Victor Gollancz.

Dziewulski, J. (1997), Interviewed by K. Różycki, *Angora*, 14 December, Poland.

Dziewulski, J. (2001), Interviewed during an Internet chat, available at: http:/czateria.interia.pl/gosc?cid+633&F=5.

Edelman, M. (1964), *The Symbolic Uses of Politics*, University of Illinois Press, Illinois.

Eggen, D. (2002), 'Ashcroft Assailed on Policy Review', *Washington Post*, 21 August.

Eggen, D. and Pincus, W. (2005), 'Bush Approves Spy Agency Changes, *Washington Post*, June 30.

Eisendrath, C. (2000), 'Introduction', in C. Eisendrath (ed.), *National Insecurity: US Intelligence after the Cold War*, Philadelphia: Temple University Press, pp. 1–7.

Electronic Privacy Information Centre, *The Year Books,* available at: http://www.epic.org.

Evenimentul Zilei (2002a), 'Iliescu si Nastase se bat pe serviciile secrete: Potrivit institutul britanic Oxford Analytica' [Iliescu and Nastase fight for the secret services: According to the British institution Oxford Analytica], *Evenimentul Zilei*, 3 June.

Evenimentul Zilei (2002b), 'Emil Constantinescu: Securistii epurati de mine sint de azi patroni de ziare' [Emil Constantinescu: The Securitate lustrated by me are today the patrons of newspapers], *Evenimentul Zilei*, 4 October.

FAC (2003), *The Decision to go to War in Iraq*, Ninth Report of Session 2002–2003, HC813-I, The Stationery Office Limited, London.

Farson, S. (2005), 'The Delicate Balance Revisited: Parliamentary Democracy, Intelligence, and the War against Terrorism in Canada', in H. Born, L. Johnson, and I. Leigh (eds), *Who is Watching the Spies? Establishing Intelligence Service Accountability*, Brasseys, Dulles, VA.

FAS Secrecy News (2004), Issue No. 43. May 7.

Faupin, A. (2002), *Reform of the French Intelligence Services After the End of the Cold War*, Paper presented at the Workshop on Democratic and Parliamentary Oversight of Intelligence Services, Geneva, 3–5 October, available at: http://www.dcaf.ch/news/Intelligence%20Oversight_051002/ws_papers/Faupin.pdf.

Favier, P. and Martin-Roland, M. (1991), *La Décennie Mitterrand, Vol. II: Les Epreuves* [The Mitterrand Decade: The Ordeals], Vol. II: Paris, Seuil.

Federation of American Scientists (1997), *Intelligence Resource Programme*, available at: http://www.fas.org/irp/world/france/defense/drm/index.html.

Finckenauer, J. and Waring, E. (2000), 'Russian Emigré Crime in the United States: Organised Crime or Crime that is Organised', in P. Williams (ed.), *Russian Organised Crime: The New Threat*? Frank Cass, London-Portland, 2nd edn, pp. 139–155.

First Report from the Home Affairs Select Committee for 1992–1993 (1993), *Accountability of the Security Service*, HC 265, United Kingdom.

Flaherty, D. H. (1989), *Protecting Privacy in Surveillance Societies*, University of North Carolina Press, North Carolina.

Foreign Affairs Committee (2003), *The Decision to go to War in Iraq*, ninth Report of Session 2002–2003, HC813-I, The Stationery Office Limited, London.

Foreign Intelligence Agency (2003), *Supervision of the Prime Minister over the Foreign Intelligence Agency Operations*, Foreign Intelligence Agency, available at: http://www.aw.gov.pl/eng/kontrola/prezes-rady-ministrow.html.

Frączak, P. (2002), *Trzeci sektor w III Rzeczypospolitej* [Third Sector in Post-Communist Poland], Fundusz Współpracy, Warsaw, Poland.

Franks, C.E.S. (1989), 'Accountability for Security Intelligence Agencies', in *National Security: Surveillance and Accountability in a Democratic Society*, P. Hanks and McCamus J. (eds), Les Editions Yvon Blais, Inc., Cowansville, Quebec, pp. 4.

Frykowski, M. (2003*), Wyznaczniki zaufania społecznego mieszkańców Łodzi* [Indicators of social trust among dwellers of the city of Łódź], Thesis (PhD), University of Łódź, Poland.

Galleotti, M. (2002), 'Intelligence sharing in a wider NATO', *Jane's Intelligence Review*, 1 July, available at: http://www.janesonline.com.

Garapon, A. (2005), 'Is there a French Advantage in the Fight Against Terrorism?, *International Terrorism,* Ari Nr. 110/2005, 09 September, available at: http://www.realinstitutoelcano.org/analisis/807/Garapon807.pdf.

Gargas, A. (1997), 'Ludzie FOZZ' [People of FOZZ {FOZZ name of the most notorious economic scam in Post-Communist Poland], *Gazeta Polska*, 20 February, p. 4, Poland.

Gargas, A. (2002), 'Zemsta' [Revenge], *Gazeta Polska*, 12 June, pp. 3, 6, Poland.

Gargas, A. (2003), 'Imperium zielonych cieni' [Empire of green shadows], *Gazeta Polska,* 9 July, pp. 3–5. Poland.

Garton Ash, T. (2006), 'The Twins' New Poland', *The New York Review of Books*, 53(2), 9 February 2006.

Georgescu, R. (2001), 'Radu Timofte a fost acuzat ieri in plenul Parlamentului ca a colaborat cu KGB' [Radu TImofte was accused yesterday in the parliamentary plenum of having collaborated with the KGB], *Romania Libera*, 8 February, Romania.

Gieseke, J. and Hubert, D. (2002), *The GDR State Security: Shield and Sword of the Party*, The Federal Commissioner for the Records of the State Security Service, Berlin.

Gill, P. (1991), 'The Evolution of the Security Intelligence Debate in Canada since 1976', in A.S. Farson, D. Stafford and W. Wark (eds), *Security and Intelligence in a Changing World*, London: Frank Cass., pp. 75–94.

Gill, P. (1994), *Policing Politics: Security Intelligence and the Liberal Democratic State*, Frank Cass, London.

Gill, P. (1996), 'Reasserting Control: Recent Changes in the Oversight of the UK Intelligence Community', *Intelligence and National Security*, 11(2), pp. 313–31.

Gill, P. (2004), 'Securing the Globe: Intelligence and the Post-9/11 Shift from 'Liddism' to 'Drainism', 19 *Intelligence and National Security.*

Gill, P. (2005), 'The Politicisation of Intelligence: Lessons from the Invasion of Iraq', in H. Born, L. Johnson, and I. Leigh (eds), *Watching the Spies: Maintaining Accountability Over the World's Secret Intelligence Agencies*, Potomac Books Inc., Washington DC., pp. 12–33.

Gill, P. (forthcoming), 'Keeping in Touch with "Earthly Awkwardness": Failures of Intelligence Analysis and Policy in the UK', in T. Bruneau and K. Dombrowski (eds), *Reforming Intelligence Across the World: Institutions and Cultures*, University of Texas Press, Austin.

Gillan, A. (2003), 'Torture Testimony "acceptable"', *The Guardian*, July 22.

Giménez-Salinas, A. (2003), 'The Spanish Intelligence Services', in J.-P. Brodeur *et al.* (eds), *Democracy, Law and Security: Internal Security Services in Contemporary Europe*, Ashgate, Aldershot.

Glees, A. (2004), 'Evidence-Based Policy or Policy-Based Evidence', *Parliamentary Affairs*, vol. 58(1), p. 138.

Glees, A. and Davies, P. (2004), *Spinning the Spies: Intelligence, Open Government and the Hutton Inquiry*, Social Affairs Unit, London.

Glees, A., Davies, P. and Morrison, J.(2006), *The Open Side of Secrecy: Britain's Intelligence and Security Committee*, (Social Affairs Unit, London 2006).

Gormley, D. M. (2004), 'The Limits of Intelligence: Iraq's Lessons', *Survival* 46:3 Autumn, pp. 7–28.

Gottesman, K. (2003), 'Błąd z konsekwencjami' [A mistake of consequences], *Rzeczpospolita*. 23 January, Poland.

Grajewski, A. (1996), 'Lustracja po polsku' [Lustration – the Polish way], *Przegląd Polityczny,* No. 31, pp. 8–14, Poland.

Greenberg, K. J. and Dratel, J.L. (2005), *The Torture Papers: The Road to Abu Ghraib*, Cambridge University Press, Cambridge.

Gregory, S. (2003), 'France and the War on Terrorism', *Terrorism and Political Violence*, Vol. 15/1, Spring, pp. 123–147.

Groblewski, K. (1999), 'Ze strachu, dla paszportu, dla studiów, z wyboru' [Of fear, to get a passport, to become a university student, of free choice], *Rzeczpospolita*, 3 March, Poland.

Gumbel, A. (2003), 'America Admits Suspects Died in Interrogations', *Independent*, 7 March.

Hänggi, H. (2003), 'Making Sense of Security Sector Governance', in H. Hänggi and. T.H. Winkler (eds), *Challenges of Security Sector Governance*, Münster: Lit.

Hannant, L. (2000), 'What's in My File? Reflections of a 'Security Threat', in G. Kinsman, D. Buse and M. Steedman (eds), *Whose National Security? Canadian State Surveillance and the Creation of Enemies*, Toronto: Between the Lines.

Hastedt, G.P. (1991), 'Towards the Comparative Study of Intelligence', *Conflict Quarterly*, 11(3), pp. 55–72.

Hastedt, G.P. (1991a), 'Controlling Intelligence: Defining the Problem', in G. Hastedt (ed.), *Controlling Intelligence,* London: Frank Cass, pp. 6–8.

Hausner, J. and Marody, M. (eds) (2000), *Jakość rządzenia. EU-monitoring IV* [Quality of Governance], Kraków: Małopolska Szkoła Administracji Publicznej Akademii Ekonomicznej w Krakowie, Poland.

Hausner, J. (2003), 'Akt oskarżenia' [An indictment], *Polityka,* 21 June, pp. 38–40, Poland.

Hellman, J.S, Jones, G. and Kaufman, D. (2000), *Seize the State, Seize the Day: State Capture, Corruption and Influence in Transition*, World Bank Policy Research Working Paper No. 2444, September.

Hellman, J. and Schankerman, M. (2000), *Intervention, Corruption and Capture: The Nexus Between Enterprises and the State*, European Bank for Reconstruction and Development, Working Paper No. 58.

Helsinki Foundation for Human Rights, Warsaw and the Center for National Security Studies, Washington. 'Security Services in Civil Society: Oversight and Accountability', Report of conference held 30 June – 2 July 1995, Warsaw. Available at: http://www.hfhrpol.waw.pl/Secserv/conf_rept/index.html.

Henderson, R.D'A. (2002), *International Intelligence Yearbook, 2002 Edition,* Brassey's Inc., Washington DC.

Herman, M. (1996), *Intelligence Power in Peace and War*, Cambridge University Press, Cambridge. Polish translation: Herman, M. (2002), *Potęga wywiadu*, Dom wydawniczy Bellona Warsaw, Poland.

Hiden, M. (1973), *The Ombudsmen in Finland*, University of California Press, Berkeley.

Hill, E. (2002), *Joint Inquiry Staff Statement, Part I* [online]. House Permanent Select Committee on Intelligence and Senate Select Committee on Intelligence, September 18, available at: http://www.fas.org/irp/congress/2002_hr/091802hill.html.

Hilsman, R. (1995), 'Does the CIA Still Have a Role?', *Foreign Affairs*, 74 (5), September-October, pp. 104–116.

Hiro, D. (2005), *Secrets and Lies: the True Story of the Iraq War*, Politico's, London.

HMG (2002), *Iraq's Weapons of Mass Destruction: the assessment of the British Government*, September 24, available at: http://www.number-10.gov.uk/output/Page 271.asp.

Holt, P.M. (2000), 'Who's Watching the Store? Executive-Branch and Congressional Surveillance' in C. Eisendrath (ed.), *National Insecurity: US Intelligence after the Cold War*, Temple University Press, Philadelphia.

House of Commons. (2005), *National Security in Canada, Report of the Standing Committee on Public Accounts,* Communication Canada – Publishing, Ottawa.

Human Rights Without Frontiers (2003), *The Council of State Orders Intelligence Services to Inform a Scientologist About their Data Concerning Him*, available at: http://www.hrwf.net/html/france_2003.html#TheCouncilofStateorders.

Hutton (2004), *Report of the Inquiry into the Circumstances Surrounding the Death of Dr. David Kelly*, United Kingdom, January 24, available at: http://www.the-hutton-inquiry.org.uk.

IFJ (International Federation of Journalists) (1999), *Money, Power and Standards: Regulation and Self-Regulation in South-East European Journalism. Practices and Procedures in Albania, Bulgaria, Croatia and Romania*, European Initiative for Democracy and Human Rights, Brussels, November.

Ignatius, D. (2005), 'Can the Spy Agencies Dig Out?' *Washington Post*, April 15.

Indulski, G. (2003), 'Wojskowa Służba Iluzji' [Military Service of Illusions], *Newsweek Polska,* 29 June, pp. 30-31, Poland.

Iordache, D. (2002), 'Serviciul Roman de Informatii are pagina pe Internet' [The Romanian Intelligence Service has an internet page], *Cotidianul*, 20 July, Romania.

Iordache, M. and Castali, L. (2002), 'SRI isi face centru de Coordonare Operative Antiterorista' [The SRI is establishing a center for anti-terrorist operational coordination], *Jurnalul National*, 14 March, Romania.

IRSOP (*Institutul Roman de Sondaj si Opinia Publica*) (2002), *Sondajul IRSOP privind opinia romaniilor despre rolul si activitatea serviciilor de informatii realizat pentru televiziunea romana in perioada 16–20 martie 2002* [IRSOP poll regarding the opinion of Romanians about the role and activity of the intelligence services taken for Romanian television during 16–20 March 2002], IRSOP, Bucharest, 16–20 March.

ISC (1996), *UK Annual Report for 1995*, Cm. 3198, United Kingdom.

ISC (1998), *UK Annual Report for 1997–1998*, Cm. 4073, United Kingdom.

ISC (1999), *UK Annual Report for 1998–1999*, Cm. 4532, November, United Kingdom.

ISC (2000a), *UK Annual Report for 1999–2000*, Cm. 4897, United Kingdom.

ISC (2000b), *UK The Mitrokhin Inquiry Report*, Cm. 4764, June, United Kingdom.

ISC (2001), *Interim Report for 2000–2001*, Cm. 5126, para. 26, United Kingdom.

ISC (2002a), *Annual Report 2001–2002*, Cm. 5542, June, United Kingdom, available at: http://www.cabinetoffice.gov.uk/publications/reports/intelligence/Intelligence.pdf.

ISC (2002b), *Inquiry into Intelligence, Assessments and Advice prior to the Terrorist Bombings on Bali 12 October 2002*, Cm 5724, December, United Kingdom, available at: http://www.cabinetoffice.gov.uk/intelligence.

ISC (2003a), *Annual Report 2002–2003*, Cm 5837, United Kingdom, available at: http://www.cabinetoffice.gov.uk/intelligence.

ISC (2003b), *Iraqi Weapons of Mass Destruction – Intelligence and Assessments*, Cm 5972, September, United Kingdom, available at: http://www.cabinetoffice.gov.uk/intelligence.

ISC (2003c), *Annual Report for 2000–2004*, Cm. 5837, June, United Kingdom.

ISC (2004*), Annual Report for 2003–2004*, Cm. 6240, June, United Kingdom.

ISC (2005a), *The Handling of Detainees by UK Intelligence Personnel in Afghanistan, Guantanamo Bay and Iraq*, Cm. 6469, March, United Kingdom.

ISC (2005b), *Annual Report for 2004–2005*, Cm. 6510, April, United Kingdom.
ISC (2006), *Report into the London Terrorist Attacks of 7 July 2005*, Cm 6785.
Ishiyama, J. and Ishiyama Smithey, S. (2000), 'Judicious choices: designing courts in post-communist politics', *Communist and Post-Communist Studies* 33, no. 3, pp. 167.
Iwanicki, S. (1994), 'Gangi próbują kupować urzędników' [Gangs try of buy administration clerks], *Rzeczpospolita*, 18 August, p. 12, Poland.
Jachowicz, J. (1997a), 'Specsiódemka' [Special seven], *Gazeta Wyborcza*, 18–19 October, p. 4, Poland.
Jachowicz, J. (1997b), 'UOP – w służbie polityki?' [The Office of State Protection – in the service of partisanship?], *Gazeta Wyborcza*, 19 September, edition 3, p. 6, Poland.
Jachowicz, J. and Kęsicka, K. (1994), 'Tajne kontrolowane' [Secret and controlled], *Gazeta Wyborcza*, 22 November, p. 4, Poland.
Jakimczyk, J. (2003a), 'Agencja Bezpieczeństwa Władzy' [The Agency of Safety of the State Authorities], *Wprost*, 21 September, pp. 30–31, Poland.
Jakimczyk, J. (2003b), 'Agencja Wiernych' [The Agency of the Loyal], *Wprost*, 30 November, pp. 26–27, Poland.
Jakimczyk, J. (2003c), 'Jednostka No. 3362' [Military Unit No 3362], *Rzeczpospolita*, 16 July, Poland.
Janecki, S. (1997), 'Wojskowe Służby Interesów' [Services of Military Interests], *Wprost*, 28 December, pp. 22–23. Poland.
Janecki, S. and Mac, J.S. (2001), 'Sąd Elektromisu' [A tribunal of Elektromis {Elektromis – a company name}], *Wprost*, 18 February, pp. 26–27, Poland.
Janke, I. (1996), 'Tajni potrzebują ciszy' [Secret agents need quiet], *Życie*, 21–22 December, pp. 12–13, Poland.
Jankowski, A. and Wyszomirska, A. (2003), 'Pisanie ustaw: sztuka czy chałtura' [Writing law: and art or hack-work], *Gazeta Prawna*, 25 November, p. 22, Poland.
Joffe, A.H. (1999), 'Dismantling Intelligence Agencies', *Crime, Law & Social Change,* 32, pp. 325–346.
Joffe, A. (2000), 'Dismantling Intelligence Agencies', *Crime, Law & Social Change,* 32, pp. 325–346.
Johannesburg Principles on National Security, Freedom of Expression and Access to Information, Freedom of Expression and Access to Information (1996), U.N. Doc. E/CN.4/1996/39, available at: http://www.article19.org/docimages/511.htm.
Johnson, L.K. (1985), *A Season of Inquiry: the Senate Intelligence Investigation*, University Press of Kentucky, Lexington.
Johnson, L.K. (1989), 'Strategic Intelligence: An American Perspective', *International Perspectives on Intelligence*, Vol. 3, No. 3, Fall, pp. 299–332.
Joint Inquiry (2002), *Joint Inquiry into Intelligence Community Activities before and after the Terrorist Attacks of September 11, 2001*, Report of the US Senate Select Committee on Intelligence (107–351) and US House Permanent Select Committee on Intelligence (107–792), December (declassified version of this Report was published in July 2003).

Jordan L.J. (2005), 'Homeland Security Faces Massive Overhaul,' *San Francisco Chronicle*, June 17.

JRZ and JZ. (2003), 'Wcześniak Macierewicza' [Prematurely born action of Macierewicz], *Trybuna*, 2–3 August, p. 6, Poland.

Kaczyński, J. (1999), Interviewed by J. Kurski. *Gazeta Wyborcza,* 29 October, Poland.

Kaczyński, L. (2001), Interviewed by E. Michalik and T. Sakiewicz, *Gazeta Polska*, 11 July, p. 4, Poland.

Kamiński, A. (2003), 'Państwo aferalne' [A state of swindles], *Rzeczpospolita*, 23 November, Poland.

Kasprów, R. (1998), 'Wraca FOZZ' [FOZZ is coming back], *Życie,* 16 January, pp. 1, 5, Poland.

Kean, T.H. and Hamilton, L.H. (2004), *The 9/11 Report: The National Commission on Terroist Attacks upon the United States*, St Martin's Press, New York, available at: http://www.9-11commission.gov.

Kent, S. (1965), *Strategic Intelligence for U.S. World Policy*, Archon Books, Hamden, CT.

Kittel, B. and Marszałek, A. (2001), 'Urząd Ochrony Suskiego' [The Office of Protection of Suski], *Rzeczpospolita*, 1 March, Poland.

Knightley, P. (1988), *The Second Oldest Profession: Spies and Spying in the Twentieth Century*, W.W. Norton, New York.

Kosobudzki, T. (1998), *Bezpieka w MSZ: Służby specjalne w polityce zagranicznej RP w latach 1989–1997* [Intelligence services in Polands Foreign Policies], Wydawnictwo ELIPSA, Kielce-Warsaw, Poland.

Kuczyńska, T. (2002), 'Rządy agentów' [Secret agents govern], *Tygodnik Solidarność*, 27 September, pp. 24–25, Poland.

Lamble, S. (2002), 'Freedom of Information, A Finnish Clergyman's Gift to Democracy', *Freedom of Information Review*, No. 97, February.

Lander, S. (2004), 'International Intelligence Co-operation: An Inside Perspective', *Cambridge Review of International Affairs*, vol. 17(3).

L'Assemblée Nationale (1999), *Proposition de loi tendant à la création d'une délégation parlementaire pour les affaires de renseignement* [Bill aiming at the establishment of a parliamentarian delegation for Intelligence Affairs], Document No. 1497, 25 March.

*Le Figaro*, 'Renseignements: Sarkozy pour un contrôle Parlementaire' [Information: Sarkozy for Parliamentary Control], 25 November 2005.

Leigh, I. (2002), 'The Legal Norms of the Geneva Centre for the Democratic Control of Armed Forces (DCAF) and Security Sector Reform', in *5th International Security Forum 'Setting the 21st Century Security Agenda'*, Zurich, 14–16 October.

Leigh, I. (2003), *Democratic Control of Security and Intelligence Services: A Legal Framework*, DCAF Working Paper No. 119, May.

Leigh, I. and Lustgarten, L. (1994), *In From the Cold: National Security and Parliamentary Democracy*, Clarendon Press, Oxford.

*Le Monde* (2002), 'L'Elysée accuse les services secrets d'avoir enquêté sur M. Chirac sous le gouvernement de M. Jospin' [The Elysée Accuses the Secret Service with Investigating M. Chirac under M. Jospin's Government], 22 June.

*Le Monde* (2005), 'La DST et les RG dans les mêmes locaux', [The Directorate of Territorial Surveillance and Intelligence Services (working) in the same premises], 25 May.

*Le Monde*, 'L'assemblée a adopté le projet de loi antiterroriste' [The Assembly Adopts an Anti-Terrorist Bill], 29 November 2005.

Le Sénat (1999), *Proposition de loi portant création d'une délégation parlementaire dénommée Délégation parlementaire du renseignement* [Bill on the establishment of a parliamentarian delegation called Parliamentarian Delegation of Intelligence], Document No. 492, 15 September.

Le Sénat (2003), 'Le contrôle parlementaire des services de renseignement' [The Parliamentary Control of Intelligence Services], in *Les documents de travail du Sénat*, Série, Législation Comparée, No. LC 103, March.

Leszczyńska, I. and Indulski, G. (2003), 'Generalicja zgarnia kasę' [Generals catch the money], *Newsweek Polska*, 23 November, pp. 22–24, Poland.

Łęski, J. (2001), 'Szara strefa, trudna sprawa' [Grey zone, difficult case], *Gazeta Polska,* 11 July, p. 8, Poland.

Łęski, J. (2002), 'Kontrrewolucja w służbach' [A counterrevolution in the intelligence services], *Gazeta Polska*, 1 May, p. 3, Poland.

Levant, C. (2002), 'SRI a publicat pe site-ul sau lista organizatiilor teroriste' [The SRI has published the list of terrorist organisations on its website], *Evenimentul Zilei*, 25 October, Romania.

Levant, C. and Boeru, M. (2002), 'Fiul colonelului MI Gaina, prins cu droguri' [The son of Interior Ministry Colonel Gaina, caught with drugs], *Evenimentul Zilei*, 28 November.

Lichtblau, E. (2003b), 'On Terror, Doubts Anew After a Scathing Report', *New York Times*, July 25.

Łoś, M. (1995), 'Lustration and Truth Claims: Unfinished Revolutions in Central Europe', *Law and Social Inquiry*, 20 (1), pp. 117–61.

Łoś, M. (2003), 'Crime in Transition: The Post-Communist State, Markets and Crime', *Crime, Law and Social Change*, *Special Issue: Crime and Markets in Post-Communist Democracies*, Vol. 40, No. 2–3, pp. 145–69, October.

Łoś, M. and Zybertowicz, A. (1999), 'Is Revolution a Solution? State Crime in Communist and Post-Communist Poland (1980–1995)', in M. Krygier and A. Czarnota (eds), *The Rule of Law after Communism: Problems and Propects in East-Central Europe*, Ashgate, Aldershot, Dartmouth, pp. 261–307.

Łoś, M. and Zybertowicz, A. (2000), *Privatising the Police-State: The Case of Poland*, Macmillan, London; St. Martin's Press, New York.

Lowenthal, M. (2000), *Intelligence: From Secrets to Policy*, Washington, DC: Congressional Quarterly Press.

Lowenthal, M. (2003), *Intelligence: From Secrets to Policy*, Washington, DC: Congressional Quarterly Press.

Lund, K. (1996), *Report to the Norwegian Parliament from the Commission appointed by Parliament to investigate allegations of illegal surveillance of Norwegian citizens (the Lund Report)*, Submitted to the Storting Presidency on 28 March 1996, Document nr 15 (1995-1996)..

Lustgarten, L. (2003), 'National Security and Political Policing: Some Thoughts on Values, Ends and Law', *Democracy, Law and Security: Internal Security Services in Contemporary Europe*, Brodeur, J.P., Gill, P and Töllborg, D., (eds), Ashgate, Aldershot, Hampshire, p. 326.

Machin, A. (2005), *Spies, Lies and Whistleblowers: MI5, MI6 and the Shayler Affair*, Book Guild Ltd, Sussex.

Macierewicz, A. (2002), 'Kursanci z Moskwy i Tel Awiwu' [Students from Moscow and Tel Aviv], *Nasza Polska*, 20 March, pp. 1, 13, Poland.

Magureanu, V. (1990), 'Report to Parliament', in *Stirea* [News], TV, TVR 1, 1990 November 27, 18:00–19:00, Romania.

Magureanu, V. (1994), Press Conference, *Romania Libera*, 1994, March 3, Romania.

Mahr, A. and Nagle, J. (1999), *Democracy and Democratization: Post-Communist Europe in Comparative Perspective*, Sage Publications, London.

Majtényi, L. (1992), *Ombudsman: Állampolgári Jogok Biztosa*, KJK, Budapest.

Maloj, J. (1998), 'Machina (nadal) postsowiecka' [The apparatus is (still) post-soviet], *Nasza Polska*, 21 January; and 13 other articles of the same author published in this weekly between February and May 1998, Poland.

Maria de Puig, L. (2005), *Report to the Parliamentary Assembly of the Council of Europe, Democratic oversight of the security sector in member states*, Council of Europe Parliamentary Assembly, Doc. 10567, 02 June, available at:
http://www.assembly.coe.int/Documents/WorkingDocs/Doc05/EDOC10567.htm.

Marszałek, A. (1998), 'Polityczne kulisy działania UOP'[The inner history of the Office of State Protection], *Rzeczpospolita*, 25 July, Poland.

Marszałek, A. (1999a), 'Agentura wśród polityków i dziennikarzy' [Secret agents among politicians and journalists], *Rzeczpospolita*, 30 October, Poland.

Marszałek, A. (1999b), 'Decyzje zapadają, wątpliwości pozostają' [Decisions taken, but doubts remain], *Rzeczpospolita*, 10 May, Poland.

Marszałek, A. (1999c), 'Trzy wywiady o UOP' [Three interviews about the Office of State Protection], *Rzeczpospolita*, 9 December, Poland.

Marszałek, A. (2001), 'Niewygodne dziennikarstwo' [Troublesome journalism], *Press*, No. 11, pp. 40–41, Poland.

Marszałek, A. (2002), 'Polska broń dla terrorysty' [Polish weapons for terrorists], *Rzeczpospolita,* 22 October, Poland.

Marszałek, A. (2003a), 'Handel pod specjalnym nadzorem' [A specially overseen trade], *Rzeczpospolita,* 23 October, Poland.

Marszałek, A. (2003b), 'Rusak potwierdza nadużycia' [Rusak (former chief of the Military Intelligence Services) confirms unlawful activities], *Rzeczpospolita,* 10 May, Poland.

McAleer, P. (2002), 'The High Cost of Free Press in Romania,' *Financial Times*, 30 September.

McCamus, J. (1989), 'Surveillance and Accountability in a Democratic Society: An Overview', in *National Security: Surveillance and Accountability in a Democratic Society*, P. Hanks and J. McCamus (eds), Les Editions Yvon Blais, Inc., Cowansville, Quebec, p. 4.

McCullagh, D. (2002), 'Report: Anti-terror Efforts Pinch Privacy,' *CNET News.com*, September 3.

McDonald, D. (1981), *Commission of Enquiry Concerning Certain Activities of the RCMP*, Three Reports (first published 1979), Minister of Supply and Services, Ottawa.

Mediafax (2002), 'SRI ingrijorat de amploarea ascultarilor ilegale: se fac interceptari prin centrale telefonice, dar si prin obiecte de uz casnic' [SRI is concerned about the extent of illegal eavesdropping: interceptions are done through the central telephone and also through the use of common household objects], *Curierul National*, 21 March, Romania.

Mendel, T. (2003), *National Security vs Openness: An Overview and Status Report on the Johannesburg Principles in National Security and Open Government*, available at: http://www.maxwell.syr.edu/campbell/opengov/Chapter%201.pdf.

Michalski, C. (2003), 'Państwo jednej partii i jednej gazety' gazety' [A country in possession of one party and one daily], *Arcana*, No. 50 (2), pp. 53–61, Poland.

Milczanowski, A. (1997), 'Bezpieczeństwo państwa i obywateli' [Security of the state and its citizens], *TransOdra*, No. 16 (Sept.), pp. 31–35, Poland.

Miller, L. (1998), Interventions in a debate 'Demokratyczna kontrola nad służbami specjalnymi' ['Democratic oversight over intelligence services], *Myśl Socjaldemokratyczna,* No 4, pp. 104–107, 123–25, Poland.

Milligan, S. (2006), 'Classified intelligence bills often unread; secret proves can discourage House debate', *The Boston Globe*, 6 August, p. A1

Mintz, J. (2003), 'At Homeland Security, Doubts Arise Over Intelligence', *Washington Post*, July 21.

Miodowicz, K. (1996), Interviewed by A. Kublik *et al.*, *Gazeta Wyborcza*, 24–25 February, pp. 10–13, Poland.

Mitchell, A. and Hulse, C. (2002), 'Accountability Concern is Raised over Security Department', *New York Times*, June 27.

MND (Ministry of National Defence) (1990), Press communiqué, 21 February, Romania.

Mönniger, M. (2004), 'A pipe smoker with a 357 Magnum', *Die Zeit*, March.

Morawski, J. (2002), 'Urząd za zamkniętymi drzwiami' [An agency behind closed doors], *Rzeczpospolita*, 6 July, Poland.

Mueller, R. (2002), Testimony of Robert S. Mueller III, Director FBI, before the Senate Select Committee on Intelligence and the House Permanent Select Committee on Intelligence, October 17.

Myrdal, G. (1968), *Asian Drama: An Inquiry Into the Poverty of Nations*, Random House, New York, 3 vols.

*Myśl Socjaldemokratyczna* (1998), 'Demokratyczna kontrola nad służbami specjalnymi' [Democratic oversight of the intelligence services. A debate], No. 4, pp. 103–125, Poland.

National Commission on Terrorist Attacks Upon the United States (2004), *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attack upon the United States*, authorised edition, W. W. Norton (New York:. Available: http://www.9-11commission.gov/report/index.htm

*Neue Züricher Zeitung,* (2005), 'Polen ohne den Mut zur Erneuerung' [Poles without courage/hope for change], 2 November.

Niemczyk, P. (1994), 'Krótka pamięć bezpieki', *Gazeta Wyborcza*, 14 November, edition waw, p. 13, Poland.

Nine O'Clock (2002), 'Intelligence services in Balkans meet periodically to exchange information', *Nine O'Clock*, 27 May, Romania.

Norwegian Parliamentary Oversight Committee (2000), Storting Report, *Document No. 16*, available at: http://www.eos-utvalget.no/Hoved/dokumentene/44/5/2000.pdf.

Norwegian Parliamentary Oversight Committee, (2001), Storting Report, *Document No. 16*, available at: http://www.eos-utvalget.no/Hoved/dokumentene/44/17/2001.pdf.

Norwegian Parliamentary Oversight Committee, (2002), Storting Report, *Document No. 16*, available at: http://www.eos-utvalget.no/Hoved/dokumentene/44/22/2002.pdf.

Ogdowski, M. (2001), *Centrale Handlu Zagranicznego jako struktury holdingowe*, Thesis (MA), Nicolaus Copernicus University, Torin, Poland.

Olbrot, A. and Subotić, M. (1997), 'Poselska korespondencja w tapczanie funkcjonariusza' [An MP's correspondence hidden by a functionary], *Rzeczpospolita,* 18 February, Poland.

Olczyk, E. and Subotić, M. (2002), 'Wszyscy ludzie premiera' [All prime-ministers men], *Rzeczpospolita*, 24 January, Poland.

Olmsted, K. S. (1996), *Challenging the Secret Government: the post-Watergate investigations of the CIA and FBI*, University of North Carolina Press, Chapel Hill.

O'Donnell, G. (1999), 'Horizontal Accountability in New Democracies', in *The Self-Restraining State: Power and Accountability in New Democracies*, in A. Schedler, L. Diamond and Mart F. Plattner (ed.), Lynne Rienner Publishers, Inc., London, p. 30.

Open Society Institute (2001), 'Judicial Independence in the EU Accession Process', *Monitoring the EU Accession Process: Judicial Independence*, p. 19. Available at: http://www.eumap.org/reports/content/20/001/judicial_accession.pdf.

Oprea, C. (2001), 'Directorul SRI nu a colaborat cu KGB' [The SRI Director did not collaborate with the KGB], *Curierul National*, 27 April, Romania.

Ordyński, J. (2000a), 'Polemika minister z prokuratorem' [A polemic between the minister and a prosecutor], *Rzeczpospolita*, 12 April, Poland.

Ordyński, J. (2000b), 'Wznowienie śledztwa' [The investigation resumed], *Rzeczpospolita,* 2 November, Poland.

Ordyński, J. (2003), 'Pod parasolem resortu obrony' [Protected by the defence ministry], *Rzeczpospolita*. 8 November, Poland.

PAD (2000), 'Generał Czempiński zeznawał za zamkniętymi drzwiami' [General Czempinski examined at a closed session], *Rzeczpospolita*, 23 November, Poland.

Paradowska, J. (2002), 'Pod niespecjalnym nadzorem'*, Polityka*, April 13.

Passi, S. (2002), Bulgarian National Radio, 8 August.

Peers, S. (2003), *The Exchange of Personal Data between Europol and the USA*, Statewatch Analysis No. 15, Statewatch, London.

Permanent Select Committee on Intelligence (1995), 'IC21: The Intelligence Community in the 21st Century, part XV Congressional Oversight', Staff Study*,* House of Representatives; One Hundred Fourth Congress. Washington DC. Available at: http://www.access.gpo.gov/congress/house/intel/ic21/ic21015.html.

Petcu, T. and Gheorghiu, L. (2002), 'Directorul RADET si un ofiter SRI – arestati' [The RADET Director and an SRI officer – arrested], *Cotidianul*, 6 December, Romania.

Phythian, M. (2005), 'Hutton and Scott: A Tale of Two Inquiries', *Parliamentary Affairsm* Vol. 55, No. 1.

Pietrzak, M. (2000), 'Oko na UOP' [An eye on the Office of State Protection], *Przegląd*, 23 October, p. 6, Poland.

Pincus, W. (2002), 'Lesser Intelligence Role Seen for Security Dept.', *Washington Post*, July 18.

Pincus, W. (2005), 'Negroponte Steps into Loop', *Washington Post*, May 13.

Piotrowski, P. (2003), 'Struktura Służby Bezpieczeństwa MSW 1975–1990' [The structure of the Security Service], *Pamięć i Sprawiedliwość,* No. 1 (3), pp. 51–107, Poland.

Pipes, D. (2005), 'Weak Brits, Tough French', *New York Sun*, July 12.

Pitts, J. (2007), 'Under Surveillance: The End of Domestic Spying? Don't Count on It', *The Washington Spectator (online)*, 15 March 2007.

PM (1998), *Government Response to the Intelligence and Security Committees Annual Report 1997–1998*, Cm. 4089.

PM (2000a), *Government Response to the Intelligence and Security Committee Report into the Security and Intelligence Agencies' handling of information provided by Mr Mitrokhin*, Cm. 4765, June.

PM (2000b), *Government Response to the Intelligence and Security Committee's Annual Report for 1999–2000*, Cm. 5013, December.

PM (2003), *Government Response to the Intelligence and security Inquiry into Intelligence, Assessments and Advice prior to the terrorist Bombings on Bali 12 October 2002*, Cm 5765, Presented to parliament by the prime minister, February.

Podemski, A. (2002), 'Bez powtórnej weryfikacji' [No second screening], *Rzeczpospolita*¸ 15 March, Poland.

Podgórecki, A. (1993), *Social Oppression*, Westport, Con. and Greenwood Press, London.

Popa, C. (2002), 'Serviciile secrete – obligate sa puna la dispozitia PNA informatii neprelucrate' [The secret services – obliged to place raw intelligence at the disposition of the PNA], *Romania Libera*, 18 April, Romania.

Porch, D. (1995), *The French Secret Services: From the Dreyfus Affair to the Gulf War*, London: Macmillan.

Priest, D. (2005), 'Help from France Key In Covert Operations', Washington Post, 3 July.

Privacy International (2003), 'Country Report: The French Republic', in *Privacy International, Privacy and Human Rights 2003: An International Survey of Privacy Laws and Developments*, available at: http://www.privacyinternational.org/survey/phr2003/countries/france.htm.

Pyle, C. (1970), 'CONUS Intelligence: the army watches civilian politics,' Washington Monthly Magazine, January.

Pytlakowski, P. (2001), 'Republika tajnych służb' [A republic of the intelligence services], *Polityka,* 21 July, pp. 3–9, Poland.

Pytlakowski, P. (2003a), 'Koledzy z Alei Niepodległości' [Friends from the military intelligence], *Polityka*, 25 January, pp. 24–27, Poland.

Pytlakowski, P. (2003b), 'My podejrzewamy, nas podejrzewają' [We suspect, we are suspected], *Polityka*, 15 November, pp. 20–22, Poland.

Quiles, P. (2000), 'Le renseignement: zone d'ombre de la République' [Intelligence: the shady area of the Republic], *Hommes et Libertés*, No. 109, April/May.

Raport speckomisji o nielegalnym handlu bronią przez WSI [An account of the parliamentary special commission on illegal arms trade by the Military Intelligence Services] (2003), *Dziennik PAP on-line*, 31 July, available at: http://www.dziennik.pap.com.pl.

Report of a Committee of Privy Counsellors (2004), *Review of Intelligence on Weapons of Mass Destruction*, The Stationery Office, London, 14 July, available at: http://www.butlerreview.org.uk/report/.

Risen, J. (2002), 'Congress Seeks F.B.I. Data on Informer; F.B.I. Resists', *New York Times*, October 6.

Roberts, A. (2001), *Supranational Governance and the Right to Information: Lessons from Experience in the EU*, Colloquium of the Transatlantic Consortium for Public Policy Analysis and Education, September 22, available at: http://www.spea.indiana.edu/tac/colloquia/2001/pdf/roberts%20paper.pdf.

Roberts, A. (2003), *NATO's Security of Information Policy and the Right to Information, in National Security and Open Government: Striking the Right Balance*, Campbell Public Affairs Institute, Syracuse.

ROD (2003), 'Akta Bolka i zły wyrok' [The Bolek's file and a wrong conviction], *Gazeta Wyborcza – Gazeta Morska*, 12 March, p. 1, Poland.

Rosen, R. (2002), 'On the Public's Right to Know', *San Francisco Chronicle*, January 6.

Roussin, M. (1999), 'Le Parlement et les services secrets' [Parliament and the Secret Services], Le Monde, 29 December.

Rusak, T. (2003), Interviewed by E. Łosińska, *Dziennik Polski*, 12 September, Poland.

Ruzikowski, T. (2003), 'Tajni współpracownicy pionów operacyjnych aparatu bezpieczeństwa 1950–1984' [Secret collaborators of Communist security service], *Pamięć i Sprawiedliwość,* No. 1 (3), pp. 109–131, Poland.

Rzeplinski, A. (2003), 'Security Services in Poland and their Oversight', in J.P. Brodeur *et al.* (eds), *Democracy, Law and Security: internal security services in contemporary Europe*, Ashgate, Aldershot.

Sadura, E. (1997), 'Polityczny brukowiec' [A political tabloid], *Trybuna*, 28 November, pp. 10–11, Poland.

Sajo, A. (1998), 'Corruption, Clientelism, and the Future of the Constitutional State in Eastern Europe', *East European Constitutional Review*, 7(2), pp. 37–46.

Schedler, A. (1999), 'Conceptualizing Accountability', in *The Self-Restraining State: Power and Accountability in New Democracies,* in A. Schedler, L. Diamond and Mart F. Plattner (ed.), Lynne Rienner Publishers, Inc., London, pp. 14–17.

Scheeres, J. (2002), 'ACLU Acts Against Patriot Act', *Wired News*, October 16.

Schulz, H. (2003), 'Trzoda doktora Kulczyka' [Flock of doctor Kulczyk], *Nie*, 24 April, p. 6, Poland.

Seelye, K. Q. (2002), 'War on Terror Makes for Odd Twists in Justice System', *New York Times*, June 23.

Sejersted, F. (2005), 'Intelligence and Accountability in a State without Enemies: The Case of Norway', in H. Born, L.K. Johnson and I. Leigh, *Who's Watching the Spies?: Establishing Intelligence Service Accountability*, Potomac Books Inc.

Semka, P. (2003), 'Trzęsienie ziemi w Rywilandii', *Arcana*, No. 50 (2), pp. 37–52, Poland.

Serbanescu, M. (2002), 'SRI-istul Carali a fost urmarit, un an, pas cu pas' [The SRI officer Carali was followed for a year, step by step], *Adevarul*, 10 December.

Shapiro, J. and Suzan, B. (2003), 'The French Experience of Counter-Terrorism', *Survival*, Vol. 45/1, Spring, pp. 67–98.

Shanker, T. and Risen, J. (2002), 'Rumsfeld Weighs New Covert Acts by Military Units,' *New York Times*, August 12.

Shulsky, A. (2002), *Silent Warfare*, Dulles, Brassey's Inc.

Siemiątkowski, Z. (1997), Interviewed by A. Marszałek, *Rzeczpospolita*, 24 January, Poland.

Siemiątkowski, Z. (1998), An Intervention in a Debate, 'Demokratyczna kontrola nad służbami specjalnymi' [Democratic oversight of the intelligence services], *Myśl Socjaldemokratyczna*, No. 4, pp. 107–13, Poland.

Siemiątkowski, Z. (2001), Interviewed by M. Barański, *Nie*, 26 July, p. 5, Poland.

Silberman, L. and Robb, C. (2005), *The Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction*, Report to the President, March 31, available at: http://www.wmd.gov/report/wmd_report.pdf.

Sima, O. (2001), 'Virgil Magureanu pune pe tapet a noua problema: scurgerile din cadrul Serviciul Roman de Informatii' [Virgil Magureanu places a new problem on the table: the information leaks from within the Romanian Intelligence Service], *Curierul National*, 26 April, Romania.

SIRC (2002), *Report 2001–2002: an Operational Audit of the Canadian Security Intelligence Service*, Public Works and Government Services Canada, Ottawa.

Skłokowski, T. and Woyciechowski, P. (1997), 'Agenci bez przydziału' [Agents with no assignment], *Rzeczpospolita*, 19 November, Poland.

Skórzyński, J. (ed.) (2003), *System Rywina, czyli druga strona III Rzeczypospolitej* [The Rywin System: Or the second side of Post-Communist Poland], Warszawa: Świat Książki I, *Rzeczpospolita*, Poland.

SLD – Rada Krajowa (2001), 'Zespół ds. Cywilnej i Demokratycznej Kontroli Służb Specjalnych' [Team for civilian and democratic oversight of intelligence services], *Opcja 2001: przyszłość polskich służb specjalnych*, Warszawa: Instytut Problemów Bezpieczeństwa Fundacja Naukowa, Poland.

Smith M. (2005a), 'Blair hit be new leak of secret war plan,' *Times*, May 1.

Smith M. (2005b), 'The Real News in the Downing Street Memos,' *Los Angeles Times*, June 23.

Smolar, A. (2000), 'Lustracja na naszą miarę' [Lustration that fits us], *Gazeta Wyborcza*, 24 January, pp. 15–17, Poland.

South Africa History Archive (2002), Conference report of 'Unlocking South Africa's Nuclear Past', available at: http://www.wits.ac.za/saha/programmes_foip_03_nuclear1.htm.

Sparrow A. (2004), 'Not our job to bring down Blair, says Butler,' *Daily Telegraph*, October 22.

SRI (2002a), *Material: Personnel Evolution of Department for State Security, December 1989*, Human Resource Department, Romanian Intelligence Service, July, Romania.

SRI (2002b), The National Strategy on Preventing and Combating Terrorism, Bucharest: Romanian Intelligence Service, Romania.

SRI (2002c), Pericolul Interceptarii illegal a comunicatilor: documentar [The danger of illegal interception of communications], Romanian Intelligence Service, available from http://www.sri.ro, Romania.

SRI (2002d), SRI Annual Report 1990, Press Bureau, 2002 September, Romania.

SSCI (2004), *Report on the US Intelligence Community's Pre-War Intelligence Assessments on Iraq*, July 7, available at: http://intelligence.senate.gov.

Stachowiak, J. (2000), 'UOP listy czytał' [The Office for State Protection was reading the mail], *Gazeta Wyborcza*, edition Poznań, 24 February, p. 1, Poland.

Stan, I. (2002), Parliamentary Oversight of the SRI, Unpublished paper, 15 July.

Stankunowicz, E. (2000), 'Widmo nowych elit' [A specter of new elites], *Businessman Magazine*, No. 7(July), pp. 18–24, Poland.

Staniszkis, J. (1999), *Post-Communism: The emerging enigma,* Warsaw: Institute of Political Studies, Polish Academy of Sciences, Poland.

Staniszkis, J. (2001), *Postkomunizm. Próba opisu* [Post-Communism: An attempt at portrayal], Gdańsk: słowo/obraz terytoria, Poland.

Stefan, G. (2001), Destituiri si treceri in rezerva in randul generaliilor si coloneilor SRI: Diviziunea B Contraspionaj a fost folosita in scopuri politice [Dismissals and retirements in the ranks of the SRI generals and colonels: Division B Counterespionage was used for political aims], *Adevarul*, 16 May, Romania.

Stevenson, R.W. and Shanker T. (2004), 'Ex-Arms Monitor Urges and Inquiry on Iraqi Threat,' *New York Times*, January 29.

Stevenson, W. (2000), *A Man Called Intrepid,* The Lyons Press, Guildford, CT.

Stout, D. (2004), '9/11 Panel Chiefs Signal Willingness to Bend', *New York Times*, 11 August.

STHS (2002), *Counterterrorism Intelligence Capabilities and Performance Prior to 9/11*, Report of the Subcommittee on Terrorism and Homeland Security of the House Permanent Select Committee on Intelligence, July.

STS (2002a), *Raport privind activitatea desfasurata de Serviciul de Telecomunicatii Special pe anul 2001 si principalele directii de actiune pe anul 2002* [Report on the activity of the Special Telecommunications Service during 2001 and the principal directions of its activity for 2002], Bucharest: Special Telecommunications Service, pp. 1–7. Romania.

STS (2002b), *Medium and Long Term Strategy for Special Telecommunications*. Bucharest: Special Telecommunications Service, pp. 1–25, Romania.

Sturtevant, M. (1992), 'Congressional Oversight of Intelligence: One Perspective', *American Intelligence Journal*, Vol. 13, No. 3, Summer 1992, pp. 17–20, available at: http://www.fas.org/irp/eprint/sturtevant.html.

Szikinger, I. (2003), 'National Security in Hungary', in J.P. Brodeur *et al.* (eds) *Democracy, Law and Security: internal security services in contemporary Europe*, Ashgate, Aldershot.

*The Times* (2005), 'Mitterrand Ordered the Bombing of the Rainbow Warrior, Spy Chief Says', 11 July.

*The Warsaw Voice* (2006), 'WSI Liquidated' 31 May, available at: http://www.warsawvoice.pl/view/11506.

Timofte, R. (2002a), Press conference of SRI Director Radu Timofte on occasion of NATO-MAP conference, *Intelligence and Security Services and the Security Agenda of the 21st Century*, Sinaia, 10–14 April, Romania.

Timofte, R. (2002b), 'Remarks', in *Romania Politica*, TV Romania International. 2002 March 23, 1800–2100 hrs, Romania.

Toma, D. and Hogea, O. C. (2001), Directorul SRI a fost lucrat de sefii contraspionajului [The Director of the SRI was targeted by the chiefs of counterespionage], *Cotidianul*, 16 May, Romania.

Treverton, G. (2003), *Reshaping National Intelligence for an Age of Information*, Cambridge University Press, Cambridge.

Tudor, R. (2002), Filiera RADET-SRI: PNA a arestat la sesizarea Directiei de Securitate Interna a SRI [The RADET-SRI sting: the PNA made arrests based on information from the Internal Security Directorate of the SRI], *Ziua*, 6 December, Romania.

UK Public Records Office (1999), *The Security Service 1908-1945, The Official History*, London.

UK Home Affairs Select Committee (1999), *Accountability of the Security Service*, June, HC291.

UNDP (2002), 'Deepening Democracy in a Fragmented World', Human Development Report 2002, available at: http://www.undp.org/currentHDR_E/.

US Department of State (2005), *Country Reports on Terrorism* Office of the Coordinator for Counterterrorism, April, available at: http://www.state.gov/s/ct/rls/45388.htm.

United States Senate (1976), *Final Report*, Select Committee to Study Governmental Operations with Respect to Intelligence Activities (The Church Commission), 94th Cong., 2nd Session, Rept., 94–755, May.

United States Congress, House of Representatives (1996), Permanent Select Committee on Intelligence, House of Representatives, *IC21: The Intelligence Community in the 21st Century, Staff Study*, 104th Congress, Chapter XV on Congressional Oversight, available at: http://www.access.gpo.gov/congress/house/intel/ic21/ic21_toc.html.

United States Congress, House of Representatives (1976), *Recommendations of the Final Report, House Select Committee on Intelligence,* House Report 94-883, 94th Congress, 2nd Session, Committee Print, Washington D.C.

United States Senate (1973), *Military Surveillance of Civilian Politics, A Report of the Subcommittee on Constitutional Rights,* Committee of the Judiciary, 93rd Congress, 1st Session, Committee Print, Washington D.C.

United States Senate, (1994), *Legislative Oversight of Intelligence Activities: The US Experience, Report of the Select Committee on Intelligence,* 103rd Congress, 2nd Session, S. Prt 103-88, Washington D.C.

Venice Commission (1998), *Internal Security Services in Europe*, Report adopted at the 34th plenary meeting, Venice, 7 March.

Voiades, A. (2002), 'Presa – si criticata, si cu banii luati: investitori straini acuza, in Financial Times, ziarele romanesti de santaj' [The Press – both criticized and taking money: foreign investors accuse Romanian newspapers of blackmail in the Financial Times], *Cotidianul*, 1 October.

Walaszczyk, M. (2003), 'Kariery Ireneuszów z SB' [Careers of former Communist Security Service men], *Nasz Dziennik*, 31 January, pp. 1, 3, Poland.

Wark, W.K. (2001), 'The Access to Information Action and the Security and Intelligence Community in Canada', *Report 20 – Access to Information Review Task Force*, August.

Warner, M. (2002), 'Wanted: A Definition of Intelligence', *Centre for the Study of Intelligence, Studies in Intelligence*, Vol. 46, No. 3, available at: http://www.cia.gov/csi/studies/vol46no3/article02.html.

Wassermann, Z. (2002), Interventions in a discussion. *Nowe Państwo*, No 1 (Jan.), pp. 16–20, Poland.

Waterman, S. (2005), 'Analysis: WMD panel threatened resignations', *UPI/ Washington Times*, April 15.

Watts, L. (2001), Reform and Crisis in Romanian Civil-Military Relations 1989–1999, *Armed Forces and Society*, 27, No. 4 (summer), pp. 597–622.

Watts, L. (2004), Conflicting Paradigms, Dissimilar Contexts: Intelligence Reform in Europe's Emerging Democracies, *Studies In Intelligence*, 48, No. 1, pp. 11–25.

Welch, M. (2003), 'Trampling Human Rights in the War on Terror: Implications to the Sociology of Denial', *Critical Criminology*, Vol. 12, pp. 1–20.

Weller, G. (2000), 'Political Scrutiny and Control of Scandinavia's Security and Intelligence Services', *International Journal of Intelligence and Counterintelligence*, 13 (2), pp.171–192.

Wesley Pue, W. (2000), 'Policing, the Rule of Law, and Accountability in Canada: Lessons from the APEC Summit', *Pepper in Our Eyes: The APEC Affair*, W. Wesley Pue (ed.), UBC Press, Vancouver and Toronto, pp. 20–21.

Whitaker, R. (1999), 'Designing a Balance between Freedom and Security', in J. Fletcher (ed.), *Ideas in Action: Essays on Politics and Law in Honour of Peter Russell*, Toronto, University of Toronto Press, pp. 126–149.

Whitaker, R. (2002), 'A Poor Bargain', *New Scientist*, 174, June 29, p. 26.

Whitelaw (2005), 'National Security Watch: A Portrait of CIA-FBI Dysfunction', *US News*, June 16.

Widacki, J. (1992), *Czego nie powiedział generał Kiszczak* [What wasn't told by gen. Kiszczak], BGW, Warsaw, Poland.

Widacki, J. (1999), 'System bezpieczeństwa wewnętrznego – ewolucja struktur i funkcji' [System of internal security – an evolution of structures and functions], in L. Kolarska-Bobińska (ed.), *Druga fala polskich reform* [Second wave of Polish reforms], Instytut Spraw Publicznych, Warsaw, Poland, pp. 215–48.

*Więź* (2000), 'Co się stało z państwem policyjnym?' (a debate) [What has happened to the police-state], No. 10, Poland, pp. 43–64.

Wilczak, J. (2000), 'Szwindel-Mielec: Pod bokiem kontrwywiadu skradziono lotnisko' [Swindle-Mielec: An airfield stolen while the counterintelligence was watching], *Polityka*, 20 May, pp. 35–6, Poland.

Wilczak, J. (2003), 'Niesłychanie tajna służba' [Amazingly secret service], *Polityka*, 14 June, pp. 24–27, Poland.

Wilson, P. (2005), 'The contribution of intelligence services to security sector reform', *Conflict, Security and Development*, Vol. 5, No. 1.

Williams, K. and Deletant, D. (2001), *Security Intelligence Services in New Democracies: The Cases of Czech Republic, Slovakia and Romania*, Palgrave Macmillan, London.

Winter, G. (2002), 'Case Against Seven Tied to Group Labelled Terrorist is Dismissed', *New York Times*, June 24.

Wojciechowski, J. (2003), 'Opinia' [An opinion], *Gazeta Prawna,* 25 November, p. 1, Poland.

Wolfe, N.T. (1992), *Policing a Socialist Society: The German Democratic Republic*, Greenwood Press, New York.

World Bank (1994), Governance: The World Bank's Experience, Washington.

Wróblewski, B. (1998), 'Podwójne fałszerstwo?' [A double forgery?], *Gazeta Wyborcza*, 21 April, p. 5, Poland.

Zalewska, L. (2003), 'Druga twarz doradcy premiera' [Second face of the prime-minister's advisor], *Rzeczpospolita*, 19 September, Poland.

Zaremba, P. (2003), 'Państwo to kto?', *Newsweek Polska,* 20 July 2003, pp. 11–14, Poland.

Zieliński, R. and MNS (2001), 'Akademia przekrętów' [An academy of swindles], *Super Express*, edition AB, 16 January, p. 3, Poland.

Zybertowicz, A. (1993), *W uścisku tajnych służb: upadek komunizmu i układ postnomenklaturowy* [In the grip of intelligence services: Collapse of Communism and a post-*nomenklatura* network], ANTYK, Komorów, Poland.

Zybertowicz, A. (1997), 'Niewidoczna władza: komunistyczne państwo policyjne w Polsce lat osiemdziesiątych' [An invisible power: The Communist police-state in Poland of the 80s], in R. Bäcker and P. Hübner (eds.), *Skryte oblicze systemu komunistycznego,* Wydawnictwo DiG, Warsaw, Poland, pp. 153-192, 244–247.

Zybertowicz, A. (1999), 'Urząd Ochrony Państwa jako podmiot gry politycznej' [The Office for State Protection as an agent of political game], *Zeszyty Naukowe WSO im. T. Kościuszki*, special issue: Socjologiczne aspekty bezpieczeństwa narodowego, Wrocław, pp. 141–155, Poland.

Zybertowicz, A. (2002a), 'Demokracja jako fasada: przypadek III RP' [Democracy as a facade: The case of Post-Communist Poland], in E. Mokrycki, A. Rychard and A. Zybertowicz (eds), *Utracona dynamika? O niedojrzałości polskiej demokracji* [The lost dynamics? On immaturity of the Polish democracy], IFiS PAN, Warsaw, Poland, pp. 173–214.

Zybertowicz, A. (2002b), 'Odwrócone spojrzenie: czy służby specjalne znajdują się marginesie transformacji ustrojowej?' [Averted look: do intelligence services make an impact on the systemic transformation], *Colloquia Communia*, No. 2 (73) July-December, pp. 233–249, Poland.

Zybertowicz, A. (2005), '*An Unresolved Game: The Role of the Intelligence Services in the Nascent Polish Democracy*, in H. Born, L.K. Johnson and I. Leigh, *Who's Watching the Spies?: Establishing Intelligence Service Accountability*, Potomac Books Inc., Dulles, Va.

# Index

Table are indicated by bold page numbers, figures by italic.