Technology and Anti-Money Laundering

Technology and Anti-Money Laundering

A Systems Theory and Risk-Based Approach

Dionysios S. Demetis

Associate Staff, London School of Economics, UK

Edward Elgar
Cheltenham, UK • Northampton, MA, USA

Published by
Edward Elgar Publishing Limited
The Lypiatts
15 Lansdown Road
Cheltenham
Glos GL50 2JA
UK

Edward Elgar Publishing, Inc.
William Pratt House
9 Dewey Court
Northampton
Massachusetts 01060
USA

A catalogue record for this book
is available from the British Library

Library of Congress Control Number: 2010922138

ISBN 978 1 84844 556 7

Printed and bound by MPG Books Group, UK

Contents

Figures

Tables

Preface

The ideas behind this book were developed gradually over a number of years. Many individuals have influenced this effort, particularly by sharing their own experiences on anti-money laundering (AML). However, what has undoubtedly taken a much longer time to establish was the connection between anti-money laundering as a pragmatic problem domain and systems theory as a theory that could be used to develop AML research. Even though this book constitutes an academic endeavour in its core, there are indeed important implications for practitioners. Research results from a financial institution that was studied over a period of three years are included in this book. I trust that the analysis of AML operations of the financial institution will be of considerable interest to the reader. This analysis is presented as an in-depth case study and a whole chapter is dedicated to this purpose. The influences of information systems on AML, as well as the internal suspicious transaction-reporting regime of the financial institution, yield some interesting results and point to a fascinating complexity around AML.

I would like to thank a number of people without whom my AML experience would not have been the same. From the London School of Economics, I would like to thank James Backhouse and Bernard Dyer, two close collaborators with whom I've worked on two AML projects funded by the European Commission (projects Spotlight and GATE), as well as Jeannine McMahon for managing these projects on behalf of LSE Enterprise. For their collaboration throughout these projects, I would like to thank a good friend and ex-student from the LSE, Giorgos Panousopoulos, as well as Massimo Nardo from the Central Bank of Italy who has always assisted our LSE-based research activities with his experience on the modelling of money laundering. For originally introducing me to systems theory, I would like to thank Ian Angell, my former PhD supervisor and co-author on a number of academic publications (including a book titled *Science's First Mistake*); he has always given me invaluable advice on a number of research initiatives and was always willing to review my work. I would also like to thank Jannis Kallinikos for pointing me to the works of Niklas Luhmann and second-order cybernetics, as well as Carsten Sørensen for a number of useful discussions on data mining applications and general discussions on technology matters.

I'm particularly grateful to Professor Ian Angell, Bernard Dyer, Professor Michael Mainelli and Alexei Poulin for reviewing draft chapters of this book and for providing me with very useful comments that have improved the text. Naturally, I would like to thank all the employees of the financial institution who have shared with me a wealth of information but who cannot be named for confidentiality reasons. This book is dedicated to them.

Dionysios S. Demetis

Abbreviations

AML:	Anti-Money Laundering
CFSP:	Common Foreign and Security Policy
CMS:	Case Management System
EU:	European Union
EUS:	Electronic Updates System
FATF:	Financial Action Task Force
FIU:	Financial Intelligence Unit
FTEM:	Fast Transmission of Electronic Messages
IMF:	International Monetary Fund
IS:	Information Systems
KYC:	Know Your Customer
LEA:	Law Enforcement Agency
ML:	Money Laundering
MLAT:	Money Laundering Analysis Team
MLRO:	Money Laundering Reporting Officer
NCCT:	Non Cooperative Countries and Territories
OFAC:	Office of Foreign Assets Control
STR:	Suspicious Transaction Report
SWIFT:	Society for Worldwide Interbank Financial Telecommunication
TF:	Terrorist Financing
TPR:	True Positive Rate
UN:	United Nations
UNDCP:	United Nations Drug Control Programme

1. Introduction

Money laundering (ML) has long been recognized as an important contemporary phenomenon and a challenging problem area. Institutions have been organizing their responses to targeting ML for some time, however these efforts have intensified over the past two decades. Following the arbitrary connection made between the financing of terrorism and money laundering, a renewed interest in the topic has emerged within the broader agenda of dealing with security issues.

Despite the continuous efforts against ML, encouraging results have not really been witnessed; prosecutions are scarce and convictions even scarcer. Although the network of stakeholders involved in anti-money laundering (AML) has expanded due to a wide range of regulatory initiatives, such an expansion has come with a number of practical difficulties for these stakeholders (that is professions like lawyers, accountants and so on) and the regulators that are supposed to check compliance against AML legislation. For most practical purposes, it would be difficult not to accept that financial institutions remain at the forefront of the fight. Consequently, the study of how financial institutions deal with this important problem domain remains crucial. However, financial institutions do not exist in a void. They are part of a complex socio-political and economic environment that, although advancing in particularly structured ways, faces unstructured consequences.

A considerable part of this lack of structure is due to the widespread penetration of technology into traditional organizations. Technology has transformed the way we operate within an organization, but more importantly, it has created a new platform for orchestrating information-utilization and its management. Of course, technology as broadly understood has little to do with both the wider study of information systems, and the very concept of *systems* as developed and analysed in this book. Still, our dependence on technology has increased considerably, and it is evident that a technology that fails to function no longer comes to a complete halt; technology does however trigger unanticipated effects of a possibly catastrophic scale. Such effects not only undermine the operations of those stakeholders adopting technology; they also influence other stakeholders and their respective functional operations. We will come to

see how these effects permeate problem domains like AML, but also, and even worse, how they go unnoticed or become masked as an operational success. Hence, in a large number of fields (AML is no exception), society has come to rely on the functioning of technology, and has developed its own structures more and more on the basis of this precondition of reliance. This technological precondition is not just limited to AML. Financial institutions have always been technologically astute and have adapted their own organizational structures to include technological developments.

The current conditions in the broader AML domain appear to have acquired a highly unstructured complexity. This complexity is partly due to the regulatory initiatives that have spawned a myriad of reactions, and partly to the various technologies that have assisted in automating organizational processes. Such complexity is also amplified by an unrestrained opportunism shown by the software industry, which for a number of years has exploited the fact that technology was deemed by regulators as a necessary tool in the development of the fight against ML. Considerable but unplanned automation of operations for identifying suspicious transactions has resulted in a series of adverse effects for Financial Intelligence Units (FIUs), the stakeholders responsible for receiving the suspicious reports. Last but not least, the introduction of the risk-based approach with the 3rd AML Directive by the European Union (EU) has created a multitude of additional ambiguities. Even though the EU has rightly taken the step of introducing a more flexible approach, a series of difficulties and uncertainties have been introduced in how such a risk-based approach should be implemented. Financial and other institutions, as well as FIUs are having a rather difficult time making sense of this newly-born complexity that comes with the very elusive nature of risk. To put it simply, no one knows how to go about introducing, supervising and managing a risk-based approach for AML as the underlying infrastructure for doing so is simply non-existent. This is heavily supported by the popular delusion that we understand what risk is and how it can be managed. Such a strong assertion is not carried out here with the purpose of overemphasizing the problems. This section merely remains a brief introduction to the arguments that will be put forward as this book develops. The reality however also remains that feedback between FIUs and financial institutions is at a primordial state, interoperability issues are barely considered and stakeholder fragmentation as well as the sharing of intelligence is left unattended.

Within this dynamic between regulatory initiatives and technological adoption, the domain of AML is facing constant reconstruction. Much like a biological organism that encodes its own survival and evolution

within a double helix of a genetic code, the anti-money laundering *system* becomes structurally coupled with the *system of technology* with which it co-evolves. This interplay implies that the systems theoretical nature of AML and technology needs to be established and examined. Beyond the realm of technology, as it is commonly perceived, this book seeks to offer an insight into the broader effects that various information systems have within a financial institution in relation to AML. This implies that the commonly perceived technological platforms that currently affect ML, those of profiling technologies that attempt to simulate money laundering behaviour, remain but a single instance of a much larger infrastructure of various computerized information systems that have similar (if not more powerful and propagating) effects on AML.

This book sets out to examine the following issues regarding AML:

1. What theoretical description can be developed in order to describe the domain of anti-money laundering through the lens of systems theory?
2. What is the role that various information systems come to occupy within financial institutions? How do the complex interactions between various information systems employed affect AML?
3. What is the nature of the risk-based approach, and what are the problems behind any attempt to model the concept of risk?

In seeking to outline the path for answering these questions, a general literature review is provided that deconstructs the problem of money laundering, while reviewing the issue of defining ML itself, estimating the ML market, reviewing some key legislative initiatives, and outlining global AML characteristics. This general review is done in Chapter 2.

Chapter 3 presents the key theoretical principles of systems theory. These constitute the foundational basis for developing the theory further and for relating systems principles to AML.

Chapter 4 describes the empirical findings of a longitudinal case study carried out in a major financial institution in the EU-area. The various computerized information systems influences are discussed in order to ponder the second research question outlined above.

Chapter 5 analyses a number of systems theory instances that lead to a description of AML as a *system*. There is an attempt to synthesize, in systemic terms, both the domain of AML and the domain of technology, all the while examining their interplay.

The book concludes with Chapter 6 where a treatise on the risk-based approach is presented, followed by a data-mining application and a number of conclusive arguments.

2. Introduction to anti-money laundering

INTRODUCTION

In this chapter, the literature on anti-money laundering is reviewed in four distinct areas of interest. First, the problem of defining money laundering is deconstructed. Besides it being a semantic issue, the problem of definition is one of crucial importance. Using John Searle's *social construction of reality*, an effort is made to articulate a description of what money laundering is, through the very nature of money per se. The focus lies partly on the functionalities that money serves. New developments both in technology and socioeconomic structures that take advantage of such technology become responsible for shaping our preconceptions on the function of money and hence the way we define ML is affected by these dynamics.

Following this deconstruction on the nature of money and money laundering, the plethora of problems that come into existence when we try to estimate the scale of the money laundering market are discussed. Even though the attempts to estimate the ML market are deemed to be highly problematic, there appear to be reasons to suggest that the market has indeed increased.

Following the treatise on the size of the money laundering market, the major international initiatives against ML are presented in clear chronological order so that the description of their evolution is outlined. A brief description of the most important initiatives is presented and an attempt is made to categorize the major contributions stemming from these initiatives.

Finally, some features of the global AML arena are discussed. These aim at providing the reader with a broader perspective of the problems involved, as well as solidifying some of the arguments put forward. The reader is reminded that while this remains an introductory chapter, there are a number of issues raised that are connected with both the theory put forward and the examples provided later on.

THE NATURE OF LAUNDERED MONEY

In order to formulate a definition of what money laundering is, we must take into consideration the fact that ML is first and foremost a process that is dynamic and is therefore subject to considerable change. But, even though there exist a large number of typologies that create many variations through their combinatory possibilities, the dynamic nature of ML cannot be solely attributed to this aspect. The nature of money also changes. Hence, we must first consider the *nature* of the money being laundered. An examination of this characteristic is deemed of particular importance to highlight the difficulties in the domain of AML.

The way money is used and perceived today has nothing to do with the early years of banking, which preceded the discovery of coinage. The first use of money as a medium of exchange was based on commodities such as ivory, leather and gold. Banking these commodities meant storing them in warehouses and keeping track of exchanges between the parties involved. The diversity in the physical properties of the medium of exchange in ancient times meant that the value being exchanged was inherent in the medium itself. It would therefore be pointless to define money by connecting it to the physical properties of the medium of exchange (Davies, 2002). A better understanding comes from acknowledging the functions that money serves as a medium of exchange, as a means of payment and store of value.

These functions that are ascribed to money are the dominant characteristics of its constitution. If we strip money from its functionality, or cease to believe that something functions as money, then money has no meaning and therefore no functionality. Money is an institutional fact (as is marriage), sourcing from the collective intentionality that assigns – to money – the agentive functions that define its purpose (Searle, 1995). In his book titled *The Construction of Social Reality*, John Searle gives a compelling account of how institutional facts are created and he thoroughly uses the example of money. Searle argues that, in the process of creating institutional facts, a *collective intentionality* plays a fundamental role for it cannot be reduced to an individual's intentionality. Searle mentions that collective intentionality assigns a new status to some phenomenon, where that status has an accompanying function that cannot be performed solely in virtue of the intrinsic physical features of the phenomenon in question. This assignment creates a new fact, an institutional fact, and one that is created by human agreement. As Searle describes it: 'The central span on the bridge from physics to society is collective intentionality and the decisive movement on that bridge in the creation of social reality is the collective intentional imposition of function on entities that cannot perform those functions without that imposition' (ibid).

Applied to money, this brings us to the realization that money could not function as such without this collective intentional imposition. Institutions that express the aforementioned collective intentionality are those that typically impose such functions on money. These institutions have a status that is not easily contested, disputed or refuted. For instance, central banks can be seen both as the primary institutions that engage in such impositions by issuing money, and at the same time as entities with a commonly shared status. Such impositions however do not only occur within the legally defined scope of function-based utilization of money. They are also carried out in money laundering schemes like Hawala,[1] whereby a token functions as money, because the agentive functions that are ascribed to the token are recognized as such. Hence, the token that encompasses these collectively imposed functions (even if that happens in an underground market), is as good as money.

Typically three common forms are recognized when it comes to examining the nature of money (Davies, 2002):

1. Commodity money: gold or other materials.
2. Contract money: pieces of paper that promise to pay the bearer in gold or other materials.
3. Fiat money: money that is not attached to gold or other materials. They are just certificates that have resulted from a collective intentionality that has essentially allowed them to be 'functioning as money'.

It could therefore be said that the transitions that have been made from commodity to contract, and from contract to fiat money, were such that the ascribed function was gradually detached from the perceived inherent value of the medium of exchange. Interestingly enough, it took 'a stroke of genius to forget about the gold and just have the certificates' (Searle, 1995). Thus, today we are using fiat money, or money that functions as such because some institutions (like central banks) have been granted a status for expressing a collective intentionality, and can therefore impose to a particular currency, an agentive function that is widely accepted. Such an acceptance stems from the trust that is the basis of any monetary order. Fiat money seems to be the most pure expression of this, as it is *intrinsically* useless (Selgin, 1994). Hence, the entire system is based on trust and contains a paradox of any self-referential system (something which will become evident as we proceed in our discussion). For instance, in England a £50 bank note states that the Bank of England promises to pay the bearer £50 on demand. 'When a customer goes into an English bank and demands £50, what is she given? Another note with the same promise; just a piece of paper. What an amazing alchemy, only in this

case it is paper and not lead that is being transmuted into gold!' (Angell, 2008)

The next level of detachment, which is yet to occur in its full scale, is one that will detach the functionality from any physical properties of the medium (paper-issued money) and the only reference will be the functionality itself, devoid of a governmental institutional backing mechanism. Electronic money, which will have no reference to dollars, euros, pounds or yen, might well be next on the horizon, and some research has examined the possibility of privately-provided e-money that could replace government issuers (England, 2000). Even though some steps can already be witnessed in this direction, a number of barriers are evident. The pre-established base of government issuers will be hard to compete against; different e-money issuers will not be easily identifiable; the place of government in regulating these new monies is unclear. This transition will be hard because the control-oriented and will-to-power-driven governments will not easily let go. Electronic money has long ago been spotted as an enabler of a mobility that will diminish their control-abilities (Greenberg and Goodman, 1996). Furthermore, electronic money at that level of functional-detachment may considerably exacerbate ML.

With electronic money under consideration, and in connection to the ascribed functionalities of money, it could be said that money is an institutional fact that may or may not take on a physical form (that is cash, e-cash), and has a variety of collectively ascribed agentive functions that allow it to serve as a medium of exchange, a unit of account or a store of value. In addition to those functions, money is also characterized by the properties of fungibility and anonymity. Subsequently, any definition on money laundering must also encompass the nature of the money being laundered, with reference to the functionality that it serves.

Money laundering then becomes the process of trying to disguise illicit-profits in order to enjoy the use of all ascribed legitimate, standardized and commonly shared agentive functions of money while the criminal origins of the entity incorporating these functions (money) become masked.

The problem is that what functions as money nowadays is becoming radically different from what we are used to think of as money. By focusing on the agentive functions that money performs, the above definition distances ML from the physical (paper-money) or electronic (bits of information) properties of money. In short, whatever it may be that governments impose an agency of functioning as money upon, this can be laundered or made to succumb to fraudulent activities. Furthermore, an entity that may function as money but may not have government backing may also succumb to fraudulent activities as well and assist in the laundering of government-backed money.

Even though it is difficult to perceive such a differentiation, the first examples already exist and considerably test our understanding of how money functions, how it is to be regulated, or how it can open new avenues for money laundering. Online games are a good example. The concept of this type of game here is very different to the stereotype of children in front of a computer screen that merely entertain themselves. There are online games that have introduced virtual online economies with fictional currencies and have broadened the scope of the interactivity between real and virtual cash. This is because the currency they introduce online can be converted back to 'real money'. In one such game called the Entropia Universe, more than half-a-million participants interact online. This virtual game platform belongs to a broader category of games categorized as MMORPGs (Massive Multiplayer Online Role Playing Games) and profits from a turnover of more than 1.5 billion PED, with PED being the virtual currency in the online space (standing for Project Entropia Dollars). A virtual exchange rate has been introduced for the purpose of converting money back and forth into USD, with the virtual exchange rate being 10/1 (that is 10 PEDs are worth $1). One can transfer money into the virtual space, make virtual investments, and transfer virtual money between residents of the virtual space. With the introduction of a real ATM card, from which the holder can withdraw money from any regular ATM, things get even more complicated since the money actually resides in virtual space (in virtual currency) and the conversion is done automatically through the virtual exchange rate.

Of course a series of issues arise when virtual games act as financial institutions and provide banking facilities. How is inflation introduced virtually by algorithms? How is the virtual economy manipulated? In all certainty, however, such evolutions are not to be taken lightly: a breakthrough investment of a real $1million to buy a virtual island took place in Project Entropia, while in the most popular MMORPG, called 'Second Life', more than $1.5 million of real currency is changing hands every day (Spiegel, 2007).

In China, virtual currency has exploded as a phenomenon through the highly popular QQ coins; this explosion has been assisted, in part, by the unpopularity of credit cards in China. As the Wall Street Journal (WSJ) reported 'a Chinese Internet company called Tencent Holdings Ltd. designed the payment system in 2002 to allow its 233 million regular registered users to shop for treats in its virtual world. Virtual currencies are in use in many countries but nowhere have they taken root more deeply than in China' (Fowler and Qin, 2007). QQ coins were originally offered for transactions of cyber-goods alone, but as their popularity increased, online marketplaces started accepting the virtual currency for real goods.

This resulted in a rapid rise of the QQ coin and prompted a reaction by the Chinese government, as circulation and trade of the real currency is strictly controlled and the government feared a destabilization of the formal currency if the effects of using QQ coins escalated. According to the WSJ article, '14 Chinese ministries and China's central bank together waged a QQ coin crackdown of sorts, calling on companies to stop trading them in order to prevent money laundering' (ibid).

This does raise the question of how the interaction between government-backed money and privately-issued money will play out. Even though the globalization of the financial system in the past few decades has meant that people could increasingly leave money overseas, the current reality of the virtual world (that is the existence of a cyberspace with which we can interact) implies that people can *increasingly leave money online*. Such money does not have to be connected to a financial institution and can change hands rapidly between digital identities of the same or different persons. The 'Know Your Customer' (KYC) cliché is replaced by the impossibility of knowing the multiple digital identities of a person. No government authorities, and no bilateral agreements can reduce this complexity effectively. People can leave money online and they can do so in virtual currencies that may have an attachment to regular monies but that – in the not so distant future – may detach themselves to have no reference to real currency whatsoever, all the while preserving the functions that allow something to function as money.

Evidently, this has nothing to do with online banking, as we currently know it. All that is required for this process is a collective intentionality and mechanisms that will establish trust amongst the collective, while at the same time disassociating it from government-backed monies. Frederick von Hayek made this point almost seventy years ago without having witnessed the explosion of internet-facilitated transactions and virtual currency. He remarked the following: 'Money does not have to be created legal tender by governments. Like law, language and morals it can emerge spontaneously. Such private money has often been preferred to government money, but government has usually soon suppressed it' (Hayek, 1978). To what extent governments will keep on suppressing such money-routes remains to be seen but if we consider how virtual currencies have been imagined and created in computer games then it becomes evident that the concept of fiat money becomes obsolete in the realm of digitization; not only is it intrinsically useless, but it also does not require a central government authority for its existence. It becomes institutionalized by the sheer propagation of its trust-base while the old institutions that gave power to former collective intentionalities (for example central banks) become eroded in this process of virtualization of money. The

collective intentionality emerges spontaneously and is unplanned by any government authority.

Even though the effect of these processes is not easy to examine, an example may shed some light on the degree of complexity that these virtual currencies have opened; a complexity that gives a whole new dimension to the concepts of economic divide, labour exploitation and outsourcing. For any individual to participate in these online gaming-economies, a digital representation of that individual's self is required. Such a digital representation has a distinct virtual identity, a set of characteristics defined according to the user and conforms to the rules of each game. The 'digital representation of self' in an online gaming platform is encapsulated in the concept of an *avatar.* If you as a user/investor want to participate in such an online virtual economy then you have to create the digital representation of yourself; you have to create your avatar. In theory, this is supposed to be a one-to-one relationship: one person, one avatar. But since the avatar is created electronically, there are no bounds to how many avatars can be created by the same person. Also, since there are plenty of virtual economies in existence, it means that one individual can have multiple avatars under their control. A recent study from the EU-funded network titled the 'Future of Identity in the Information Society' illustrates the complexity behind these processes (FIDIS, 2009).

Every avatar in an MMORPG has to go through certain stages of evolution, which require hours of participating in the online economy/game. The more skilled the avatar becomes the better equipped it is to perform a function within the online economy. The solution to those who wanted to avoid these painstaking initial processes was simple enough. Their digital identity (avatar) was outsourced to India, China, Pakistan or any other developing country. Another user with a broadband connection would take control of the avatar and would spend weeks or months to perfect the capabilities of that avatar. In return, they would receive a few dollars a day for their online labour and when they brought the avatar up to a certain standard they would pass over its control (that is the control of its identity) to its original creator who could then invest serious money in the online economy, its virtual stock market, or any other trading activity that takes place online. Another route for the exchange of digital identities was then discovered. Users would spend a great amount of time building the skills of an avatar so that it may successfully participate in an online economy and then they would auction the identities of avatars in websites that acted as identity-brokers. Similar to eBay but with virtual identities instead of tangible goods; virtual identities that could then be used to handle virtual cash, and virtual cash that could in turn be converted to real cash, anytime, anywhere.

With such evolutions occurring in the handling of money, and leading on to further avenues for ML, it is interesting to take a step back and consider the ontological constructs of criminality, and to examine what are those offences that are considered as criminal and can be associated with the laundering of money they acquire illegally. Even though it is beyond the purposes of this book to delve into such issues, their importance cannot be over-emphasized. Because of the differences between nation states in their definitions of what criminal offences are, launderers are given an advantage, an argument that has been articulated in some detail in a number of international forums. A clear example can be found in the application of *Council Directive 91/308/EEC* in different member states of the EU when it was first introduced. As the – now obsolete – directive gave flexibility on its application to national laws, it was inevitable that discrepancies and differences would follow. Launderers were thus given the opportunity to shop around for a member state with more lenient laws on detection and punishment (Mohamed, 2002). Take into account the possibilities opened up in the virtual world, and the difficulties become insurmountable. Where has the crime taken place? In the user's home computer, in the server hosting the virtual service, or in the myriad different routers that participate in the trafficking of internet protocols, thus perplexing the bit-trail? There comes a point where the interaction between virtual and real economy, virtual and real cash, perplex the originally prescribed function of anti-money laundering to act as a force against ML and complicate the money-trail along with the bit-trail even more. It is this author's contention that this relationship between the money-trail and the bit-trail will spawn new forms of money laundering activity, and new forms of anti-money laundering efforts. For example, in the year 2001, the European Central Bank was in discussions with a number of technology firms in order to embed the Radio Frequency Identification (RFID) microchips in the high-denomination euro notes (Yoshida, 2001). The technology was available but the project did not materialize. Had the project come to fruition, it would have stripped money of its anonymity-function. It would have fused the money-trail with the bit-trail and every banknote embedded with an RFID chip would carry its own record. This would have fundamentally changed the nature of fiat money and it would have created an entire new generation of money laundering through mixed techniques of both an electronic and a physical nature. Essentially, it would have created a generation of hackers that would attempt to compromise the embedded bit-trail of fiat money.

In any event, once successful, ML gives the opportunity to criminals, besides distancing themselves from the crime and the profits, to enjoy their benefits or reinvest them in order to conduct legitimate business or

fund other criminal activities (McDonell, 1998). Thus, money laundering attempts the transformation of the assets into a more usable and legitimate form, by trying to store the gained value from the criminal activities, which quite often produce large sums of money that must be manipulated (Tanzi, 1996). With the opportunities opened up by forms of cybercrime, this manipulation of money becomes further complicated. Real money can enter a virtual world (for example an online economy of an MMORPG) and it can be used as an investment to buy virtual land that is then rented to other online customers. It is envisaged that money laundering, as we currently know it, will be completely different from the potential that is created for the next generation of launderers.

THE LAUNDERING PROCESS

A fundamental distinction that has to be made while attempting to define ML is that between *methods* and *processes*. Viewing ML as a set of methods creates a variety of inconsistencies due to the ever-increasing ways that are used to launder money. Methods of laundering money are also known as typologies. The Financial Action Task Force (FATF), the world's only group targeting solely ML, regularly publishes listings of such typologies. Another way of defining ML is by portraying it as a process. The consensus surrounding such a definition is portrayed through the typical three-stage model:

1. The *placement* stage where the proceeds from the criminal activity enter the financial system.
2. The *layering* stage where the money launderer creates the complex set of financial transactions aimed at separating the illicit proceeds from the source, and blurring the audit trail.
3. The *integration* stage where the laundered proceeds can re-enter the financial system, appearing to be from a legitimate source and the result of normal business activities (CS, 2001).

Even though the above stages are adequate for describing the processes of traditional money laundering, cyber-laundering has altered them, and has given them a new perspective, worthy of brief mention and analysis. Electronic money, and the phenomenon of disintermediation, make it much easier for criminals to go through the placement stage, hitherto the stage where they were most likely to be detected (Gilmore, 1993). Through the use of the internet, it is possible to create an extremely complex audit trail in a very short period of time, which in a multi-jurisdictional financial

environment can render the possibility of detection minimal (Philippsohn, 2001). More importantly, ML on the internet has cut out an important method for detection (suspicious transaction reporting through face-to-face interaction). Money launderers have therefore moved into internet gambling, online casinos, prepaid debit cards, virtual economies, and so on. The potential for illegally utilizing these new possibilities has increased considerably (Hugel and Kelly, 2002).

ESTIMATING THE MONEY LAUNDERING MARKET?

One of the most difficult tasks of analysis is the estimation of the money laundering market. First, it is useful to acknowledge once again that what constitutes ML is constantly changing (Spotlight, 2006). For instance, when ML was connected to drug trafficking, estimations on the ML market were based upon the drug market. Once the norm-producing institutions like the UN expanded the scope of criminality of ML, then it became evident that estimations would increase as more proxies claimed their share in contributing to ML. In this section, it will be argued that it is beyond our capacity to formulate a clear understanding of how much money is actually being laundered, but at the same time there are several reasons to suggest that money laundering has increased. The first part implies an actual quantification process that can indicate how much money is being laundered annually while the second part implies a qualitative assessment that suggests why there has been an increase in ML.

It has been claimed that money laundering is the world's third largest market (Robinson, 1998), after the US domestic bond market, and the Eurobond market (Scholte, 1997). The International Monetary Fund (IMF) estimates the ML market to be between 2 to 5 per cent of the world's Gross Domestic Product, something that brings the estimate to between $600 billion and $1.5 trillion (Lilley, 2000). Similar estimates reaching $1.5 trillion come from an Ernst & Young report (Price, 2002). Using crime and economic statistics from various sources like the United Nations Crime and Justice database, Walker develops a model for estimating ML to around $2.85 trillion (Walker, 1998). Of course, these estimations do not account for cyber laundering.

The deviations in the estimates of the ML market become more evident when we look at how many different methodologies exist for this purpose. Indeed, these are as many as the proxies that can be used for the estimations as the number of predicate offences underpinning them. Furthermore, and as we have previously discussed, the dynamics of the

definition of ML which is evident from the evolution of legislation, clearly poses another serious problem in estimation. The issue of defining the underground economy remains unsettled, and besides being a semantic issue, it remains of fundamental importance (Tanzi, 1999). An example that clearly demonstrates the aforementioned problematic nature of estimating the ML market is that of Australia, where estimates range from 1.4 to 47.1 per cent of the GDP. This wide range demonstrates clearly that progress in estimating the size of the underground economy has been modest to say the least (ibid).

The above differences, and the fact that the special working team appointed from the FATF with the task of estimating the money laundering 'market', could not reach a conclusion and was dismantled one year later, shows how little confidence we should place in ML estimations. As the former chairman of the working group on statistics and methods, Mr Stanley Morris concluded: 'There is not at present any economic *deus ex machina* that will allow the accurate measurement of money laundering world-wide, or even within most large nations. The basis for such estimations simply does not exist' (Walker, 1999).

There are good reasons behind our incapacity to estimate ML. The dubious but obvious connection between the underground and the legitimate economies is such that little room is left for separating one from the other. Since ML distorts several economic statistical indices (Quirk, 1996), it is simply pointless to try and uncover the figure behind the underground economy. This is because the instruments used for the estimations are already distorted and entangled with the underground economy. Also, substantial sums of money from the underground economy have been used for legitimate businesses, ranging from the re-election of several US presidents, to the constitution of Stanford University (Duyne, 1998). In what ways ML contributes to what is termed as the 'real economy' remains unclear. It is therefore time to stop seeing ML and AML as separate entities that are in conflict. They are structurally coupled, and formulate an industry that is beyond good and evil.

The formulation of an industry that is beyond good and evil relies on their interconnectedness; one cannot exist or be defined without the other. Far beyond the arguments that ML is a crime and a problem (mainly sourcing from its connections to drug trafficking), there are some academic authors in the literature that do not portray ML as a problem. For instance, from a sociological perspective, Ditton and Brown argue that the very existence of money laundering could actually support the status quo because it gives to the people a feeling of fantasy equality that can be achieved through it that is actually in favour of a stabilized society whereby the structures differ. If that feeling of fantasy equality that could

be achieved through underground economies did not exist, then people would be more likely to revolt (Ditton and Brown, 1981).

In any case, it is a fallacy to consider any estimations of the underground economy as real. Rather they are only indicative of scale, if that. The most we can probably do is speculate on whether there has been an increase or decrease in the ML market, and there are at least two good reasons to suggest that ML has indeed increased. The first is the transition to the information age, and the second has to do with the economic aspect of globalization.

Cyber laundering (CL), signifies the transition of ML into the cyberspace via information technologies and the Internet. Moreover, the ongoing evolution of computer systems creates security issues that may make these systems prone to exploitation by launderers (Granville, 2003). Bothering with offshore financial centres could therefore prove pointless, once the PC has become the best washing machine, not forgetting that e-mail routing, encryption and anonymizer software can also be used by criminals (Lilley, 2000). E-banking and e-payment systems are also a fabric of CL that can be exploited by the launderers, something that ultimately renders Know Your Customer (KYC) policies, harder to apply (ibid).

CL magnifies the problem because of two interconnected reasons: the first is that the laundering phases may be carried out more easily, and the second is because dematerialized e-cash and its subsequent liquidity provide the opportunity for disintermediation, bringing the buyer and the seller into a direct relationship. However, it is difficult to say whether such transactions are 'black' or not, and what exactly their connection to the underground economy is (Angell, 2000). As long as taking the middlemen out of the equation proves more profitable (and it usually is) then there will be an inherent systemic trend towards the profitability of disintermediation.

The second element that could be considered as a reason for suggesting an increase in the ML market is the economic aspect of globalization. According to a research report from the IMF, there is a clear sign that countries that have welcomed the economic dimension of globalization by liberalizing their markets, and increasing their trading with others, have enjoyed dramatic economic benefits (Masson, 2001). When examining the relationship between the *Trade Openness* of a country and its *Real Per Capita Income*, it becomes evident that there is a strong positive correlation between the two (ibid) in the majority of countries examined. Two particular examples are China and Mexico.

There is strong evidence to support the fact that a country's openness to international trade is a very important factor for its growth. This makes a clear point that countries entering the globalization game (from

its economic standpoint), liberalizing their markets, will find major economic benefits but also increased risks due to the interconnectedness of the markets as evident from the credit crunch crisis of 2008 and 2009. Contrariwise, marginalized countries have had little or no growth, resulting in increasing poverty and inequality (WorldBank, 2001). In addition to that, the transition from the 'welfare state' to the 'competition state', followed by an intensification of capitalism, meant that state sovereignty was compromised and supra-territoriality of capital was unavoidable (Scholte, 1997). This gave rise to a supra-state-governance concerning capital matters, including ways to combat ML through the FATF's constitution.

The economic dimension of globalization cannot therefore be ignored, and it is safe to assume that it will continue to expand with more countries willing to expand their participation in the new global economy. This will subsequently result in a continuously increasing capital flow, which in turn will make it much easier for money launderers to conceal their transactions and carry out successful ML. The bigger the volume and number of transactions on a global scale, the easier it will be to launder money under that very beneficial globalized economy, as the money stream is of such astronomical magnitude that with a little caution, miscreants won't attract much attention. Establishing suspicious behaviour under an expanding nexus of complex transaction patterns becomes more and more difficult.

Integration and globalization of markets also bring underground markets closer together. An example is shell banks that have no physical presence in the country they are incorporated and licensed, and are usually a particular feature of some offshore centres that also exacerbate ML.

THE INTERNATIONAL FIGHT AGAINST ML

There have been several initiatives targeting the problem of ML, but it is beyond the scope of this book to analyse fully each and every one. Furthermore, their in-depth examination would require a comparative legal analysis, which would overshadow the purpose of this section, that being the identification of those initiatives that have made a significant contribution at a truly international level.

The purpose of this section is to review the initiatives in brief and in a chronological order, demonstrating how the definition and scope of ML has expanded, and bringing out the instruments that are being used for the prevention of ML, thus constituting the AML domain. The major initiatives regarding AML are presented in Table 2.1 in chronological order.

Table 2.1 A few of the most important initiatives targeting ML

Year	*Institution*	*Title of initiative*
1980	The Council of Europe, Committee of Ministers	Measures against the transfer and safeguarding of funds of criminal origin – Recommendation No. R(80)10 adopted by the Committee of Ministers and the Council of Europe
1988	The Basel Committee on Banking Supervision	Statement on Prevention of Criminal Use of the Banking System for the Purpose of Money Laundering
1988	United Nations	United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances *(Vienna Convention)*
1990	Caribbean Financial Action Task Force (CFATF)	The 19 Aruba Recommendations
1990	Council of Europe	Convention on laundering, tracing, seizure and confiscation of proceeds of crime *(The Strasbourg Convention)*
1991	The European Economic Commission	Council Directive *91/308/EEC* on Prevention of the use of the financial system for the purpose of money laundering
1992		The Kingston Declaration on money laundering
1994		International Conference on Preventing and Controlling Money laundering and the use of the proceeds of Crime: A global approach
1994	United Nations	Naples Declaration and Global Action Plan against Organized Transnational Crime, adopted at the World Ministerial Conference on OTC at Naples from the United Nations General Assembly *Resolution GA/49/159*
1996	Financial Action Task Force (FATF)	The Forty Recommendations
1996		The Riga Declaration on the fight against money laundering
1998	United Nations	Attacking the profits of crime: Drugs, money and laundering. A panel Discussion at the Twentieth Special Session of the General Assembly
1999	United Nations	International Convention for the Suppression of the financing of Terrorism
2000	United Nations	The United Nations Offshore Forum *Cayman Islands*

Table 2.1 (continued)

Year	*Institution*	*Title of initiative*
2000	United Nations	The United Nations Convention Against Transnational Organized Crime
2001	The Basel Committee on Banking Supervision	Customer Due Diligence for Banks
2001	FATF	The Financial Action Task Force Special Recommendations on Terrorist Financing
2001	European Community	Directive 2001/97/EC of the European Parliament and of the Council on 4 December 2001, amending Council Directive 91/308/EEC on prevention of the use of the financial system for the purpose of money laundering
2003	FATF	The revised forty recommendations
2005	European Commission	Directive 2005/60/EC of the European Parliament and of the Council on the prevention of the use of the financial system for the purpose of money laundering, including terrorist financing (also known as the *3rd Directive*)
2008	European Commission	Directive 2008/20/EC amending Directive 2005/60/EC

From all of the above initiatives, it would be useful to analyse briefly those that have made a considerable impact on the AML arena. These are chosen in terms of their scope, and therefore their attempt to encompass several areas of the problem domain at a truly international level. Even though there have been attempts from the early 1980s to address the problem (for example Council of Europe), it must be recognized that the first truly international initiative was that of the United Nations in the Convention titled 'United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances'. This convention is also known as the Vienna Convention.

The Vienna Convention

The major contribution, and something that was done for the very first time at this UN gathering was the requirement that all States should establish money laundering as a criminal offence. Even though the convention was focused on the proceeds of drug trafficking crimes (thus money laundering did not include reference to other types of crime), there was

participation from many States including major drug producers who faced the problem at a greater scale (Gilmore, 1999). ML became an extraditable offence, and the confiscation of the proceeds was also addressed. This of course did little to reduce the ironies in confiscating the proceeds of crime. The fact that the Asian Secretariat of the Financial Action Task Force is self-funded by the confiscated money remains an interesting phenomenon (ibid). In any event, the convention's breakthrough in criminalizing money laundering is clearly stated in Article 3:

> Each party shall adopt such measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally: conversion or transfer of property knowing that such property is derived from any drug trafficking offence, or from an act of participation in such offence. . . the concealment or disguise of the true nature, source, location, disposition, movement, rights with respect to, or ownership of property, knowing that such property is derived from an offence or offences established in accordance with subparagraph (a) (UN, 1988).

Focusing on drug trafficking, the Vienna Convention recognizes that such activities pose a serious threat to the welfare of human beings. Moreover, drug trafficking and laundering the proceeds of crime can also adversely affect the economic,[2] cultural, and political foundations of society.

According to the Vienna Convention, each party should adopt measures that would enable its competent authorities to identify, trace, and freeze or seize proceeds. Bilateral and multilateral treaties were also encouraged to increase effectiveness. Banking secrecy was also addressed, in order to ensure that it would not prevent any investigations. Furthermore, provisions were made in the convention to confiscate the proceeds of crime, even if their form has been altered or commingled with other property. Article 7 provided for mutual legal and other assistance between countries as obtaining evidence from abroad is critical for any ML investigation. Bilateral or multilateral agreements between countries could enhance that cooperation.

The UNDCP (United Nations Drug Control Programme) added an additional step, providing help in legislation and drafting a model law for ML, in 1993. Law enforcement agencies, which played a major role in that initiative, included the International Criminal Police Organization/ Interpol. Even though Interpol does not have an operational policing mandate, its infrastructure helps the overall effort. Interpol connects the National Central Bureau (NCB) of the participating countries through an Automated Message Switching System. Nearly 50 per cent of the messages being exchanged through that system are drug-related and of immediate interest for the fight against money laundering (Gilmore, 1999).

Financial Action Task Force

The Financial Action Task Force (FATF) is a single group that targets the ML domain. The group was constituted by the G7 in July 1989, and produced the famous 40 recommendations, which have received broad recognition as the world's standard for countering ML. Three important landmarks in the work of the FATF are: the forty recommendations in 1990, the revised forty recommendations in 2003, and eight special recommendations on Terrorist Financing in 2001.

Even though the FATF cannot pass laws, it does make recommendations that have a global reach and affect the FATF's standing as a major contributor in the fight against ML. Interestingly enough, the first version of the forty recommendations in 1990 called countries to ratify the UN Vienna Convention amongst other recommendations, and rather embarrassingly claimed that 'each country should, without further delay, take steps to fully implement the Vienna Convention, and proceed to ratify it' (FATF, 1990). Following that initiative, the UN asserted that the FATF recommendations should be recognized as the international standard against ML.[3] The support of the United Nations to the FATF was re-affirmed in the *Political Declaration and Action Plan against Money Laundering*, which was adopted at the twentieth special session of the UN general assembly. Most notably 'the Commission noted that the forty recommendations of the Financial Action Task Force. . . *remained the standard* by which the measures against money laundering adopted by concerned States should be judged' (UN, 1998b).

The Financial Action Task Force appraises its members annually. Recommendations 21 and 22 of the FATF, give the option to FATF-member countries to impose financial sanctions and adopt countermeasures against those that do not have sound AML policies. The group also produces a list of non-cooperative countries, a process also termed as blacklisting. In theory, the countries that do not have sound AML policies are those that are blacklisted. No G7 country has ever been blacklisted, for whatever reason, despite the fact that a large amount of laundered money goes through the US and the UK. Despite its attempts to combat ML, the United Kingdom has failed to provide a satisfactory answer to why there are not stringent measures on its protectorates. The thorny issue of why the UK had not promptly dismantled the legal and banking havens of the Crown Dependencies remains unsettled. The fact remains that this connection between the UK and its protectorates has crowned London as one of the major ML capitals of the world (Mohamed, 2002). A case of ML in the Cayman Islands shows how contradictory forces come into play. Four people charged for money laundering offences in the Cayman Islands

were cleared due to lack of evidence. The investigation uncovered the fact that the director of the Financial Intelligence Unit of the Cayman Islands (CAYFIN), Mr Brian Gibbs, had destroyed critical financial evidence on the case. For a long period of time he acted as a paid informer of MI6, and was desperately trying to keep his role secret (Rider, 2003).

Nauru may be a country that is a long way away from the Paris-based FATF, but for a number of years it was experiencing considerable pressure from the threat of financial countermeasures (Roule and Salak, 2003, Johnson, 2003) and so the country has attempted to take significant steps towards inclusion. These countermeasures applied by FATF members create a substantial financial burden on the business transactions of a country, which subsequently presents economic and credibility problems. Under such circumstances, most countries find it appropriate to comply.

There is a general consensus among observers that the FATF is US-dominated, and that US interests support the expansion of the group's sphere of influence. This comes as no surprise. Naylor (1994) gives a compelling account of US-domination of the financial world post-World War II, including the role of the IMF, the capital flight problem (from developing countries to the US), and so-called 'Pentagon Capitalism' (Naylor, 1994).

The reality is that the FATF has expanded, and it has become a very powerful stakeholder in the fight against ML. This is due, in no small part, to the fact that the FATF has made a big difference in combating ML, in that many countries have been influenced to improve and strengthen their AML efforts (Johnson and Lim, 2002). Non-compliance now means financial sanctions as well as severe difficulties when transacting with the world's biggest markets, which would suggest that the pressure imposed by the 'blame-and-shame' approach actually works. In fact, most of the countries blacklisted initially responded negatively, but soon recognized that improving their procedures would get them accepted. Subsequently the vast majority joined in with the international AML effort (Johnson, 2001).

However, after the terrorist attacks that took place on 11 September 2001 in New York, it was inevitable that changes in policy would rapidly follow. Expansion of the working agenda of the FATF to cover terrorist financing was something that has caused considerable problems in several ways. The original problem of defining ML was, and still is a nebulous issue (Tanzi, 1999), with the Financial Action Task Force claiming that ML was the processing of criminal proceeds in order to disguise their illegal origin (FATF, 2003). However, with terrorist financing, even that problematic definition of money laundering was twisted and distorted in a most profound way. The problems are many. First, terrorist activities are often funded by legal money. Second, banks now face considerable

amounts of stress, pressure and compliance fear because they have to check (besides the origin of money) the purpose of the transaction, and its use by the end customer. Third, Know Your Customer (KYC) principles can be seen as expanding to KYEC principles (Know Your End Customer), something that raises serious questions about civil liberties (Mohamed, 2002). This all points to the problematic nature of terrorist financing and its link to money laundering (Tupman, 2009). Banks are being forced into policing legitimate transactions that could potentially be used for terrorist purposes (ibid). Let us not forget that as the totality of the global financial system is being affected by these changes, only a very tiny fraction of the money being exchanged will be used for terrorist financing.

The Political Declaration in 1998 by the UN General Assembly

This declaration that took place at the twentieth special session, upgraded and updated the Vienna Convention through the 'Countering Money Laundering' Plan of Action. In this UN General Assembly, members reinstated their determination to combat the narcotics problem. They also encouraged all nations to adopt national ML legislation by the year 2003, adopting a new section for measures against ML (UN, 1998c).

Among the several aspects that were examined in this UN Assembly, particular emphasis was given to the issue of globalisation and how international cooperation must be fostered and strengthened in order to deal with the phenomenon in a globalized world. As the executive director of the Office for Drug Control and Crime Prevention, Professor Arlacchi, stated[4] 'globalisation has turned the international financial system into a money launderer's dream, and this criminal process siphons away billions of dollars per year from economic growth at a time when the financial health of every country affects the stability of the global marketplace' (UN, 1998a).

Several ways were discussed in this UN assembly on how international cooperation could be enhanced for combating the problem of ML more effectively in a globalized world. Multilateral information networks were brought up as networks of vital importance, and a specific example is that of the Egmont Group[5] linking different Financial Intelligence Units. There was also an expansion in offence of laundering money, which is termed 'money derived from serious crimes'.

The UN Convention Against Transnational Organized Crime in 2000[6]

Once again, the scope of this convention was very important as it was under the auspices of the United Nations. The major contribution of the convention was the adoption of a broader definition of money laundering,

which would include not only drugs but also a wide range of other criminal activity. The intention therefore of Article 6 of this convention was to expand the definition of money laundering by including all serious crimes on top of the pre-existing drug offences.

Article 6, the 'Criminalisation of the laundering of proceeds of crime', states that the application of laws must be done 'to the widest range of predicate offences for serious crime'. This is clearly defined in Article 2(b) as follows: 'Serious crime shall mean conduct constituting an offence punishable by a maximum deprivation of liberty of at least four years or a more serious penalty' (UN, 2000).

Moreover, Article 7 of the convention expanded the supervisory regime to non-bank financial institutions. This was another major contribution of the convention as it recognized there are many avenues for money laundering that go beyond the traditional banking institutions' route. According to Article 7: 'Each nation shall institute a comprehensive domestic regulatory and supervisory regime for banks and *non-bank financial institutions* and, where appropriate, other bodies particularly susceptible to money laundering. . . customer identification, record-keeping and the reporting of suspicious transactions are emphasized' (UN, 2000).

The Basel Committee on Banking Supervision

As the Basel Committee is responsible for the supervision of the banking sector, it has contributed to the AML domain through a series of initiatives. The Basel Committee became involved in AML as early as 1988 when it issued a statement on the 'Prevention of Criminal Use of the Banking System for the purpose of Money Laundering' (Basel, 1988). In that statement, the Basel Committee sought to alert the banking sector of the dangers that money laundering could present, and also set out some guiding principles that banks would have to employ (ibid).

In the work undertaken by the Basel Committee on 'Customer Due Diligence for Banks', important provisions were taken for outlining Know Your Customer principles (known as KYC principles). The Basel Committee asked the working group on cross-border banking to examine the KYC procedures in place and to draw up recommended standards that will be applicable to banks in all countries. The working group on cross-border banking is a joint group consisting of members of the Basel Committee and the Offshore Group of Banking Supervisors. It is worth noting that the Basel Committee portrayed sound KYC procedures as a critical component in the overall effective management of banking risks and not just anti-money laundering. According to the Basel Committee, there was no need to duplicate the work of the FATF[7] (Basel, 2001).

When the expansion of anti-money laundering saw terrorist financing being incorporated into the concerns of the various surrounding institutions, it became evident that the Basel Committee would also participate in the effort. In their paper on 'Sharing of financial records between jurisdictions in connection with the fight against terrorist financing', the Basel Committee stood firmly with the UN and the FATF. The focus of Basel's work in respect of terrorist financing was to improve the standards for all categories of institutions that provided financial services (Basel, 2002), focusing on KYC and customer due diligence. Particular attention was also given to how information exchange can be enhanced between a government body in one country to another, and from a financial entity in one country to its parent institution in a different country. In this work, the major ways of exchanging information are analysed. These are: Mutual Legal Assistance (MLA), communication between Financial Intelligence Units (FIU), which are based on Memoranda of Understanding (MoU), and supervisory channels.[8]

As communication received special attention in this paper of the Basel Committee, there was also an identification of several areas of future work. These included the sharing of information cross-border between host and home supervisors, practices for collecting and sharing information in the absence of an FIU, and treating financial groups as single entities for the purpose of enhancing the sharing of information within the same group (ibid).

In 'Shell banks and booking offices', the Basel Committee aims to clarify what should be the stance of the supervisory authorities when it comes to shell banks. Shell banks in the Basel document are defined as: 'banks that have no physical presence (meaningful mind and management) in the country where they are incorporated and licensed, and are not affiliated to any financial services groups that is subject to effective consolidated supervision' (Basel, 2003b).

Thus, a shell bank would have a registered agent operating in the country of incorporation, but one who would not be necessarily familiar with the operations of the bank. This creates several problems for the supervision of such structures because the supervisory authority in the country from which the bank is run may not be aware of the bank's existence. Similarly, the term 'booking branch' is analysed as one where the branch is not managed in the jurisdiction in which it is licensed. According to the Basel Committee, in such cases the home country supervisor should demand that the books and records of the branches be available. Risk management and supervision also lies with the head office (ibid).

Besides contributing to a bank's safety and soundness, KYC policies play an integral role in protecting the integrity of the banking system

and reducing the likelihood of banks becoming vehicles for ML, terrorist financing, and other illegal activities. In 'Consolidated KYC Risk Management', the Basel Committee seeks to guide banks towards a global application of the areas outlined in customer due diligence. These are: customer acceptance policy, customer identification, ongoing monitoring of higher risk accounts, and risk management (Basel, 2001). The incorporation of a consistent identification and monitoring programme of customer accounts globally is therefore vital. Customer accounts should be monitored globally, across business lines and across geographical locations (Basel, 2003a). The Basel Committee proposes two ways that such monitoring can be accomplished. The first is the use of a centralised database, and the second is decentralised databases with robust information sharing between the head office and its branches and subsidiaries (ibid).

As many banking groups engage in businesses that involve securities and insurance, sound risk management becomes more essential. This makes efficient supervision critical and the Basel Committee urges supervisors to review, besides policies and procedures, customer files, and to proceed in the sampling of some accounts. Importance is also given to internal audits whereby supervisors should seek to have access to the results of these audits (ibid).

Council Directive 91/308/EEC on Prevention of the Use of the Financial System for the Purpose of Money Laundering (Amended by Directive 2001/97/EC)

The first European initiative was much earlier than this directive, with the Council of Europe Convention on 'Measures against the Transfer and Safekeeping of Funds of Criminal Origin'. The 1980 convention focused on KYC principles, training and other aspects, but it was the 1990 Council of Europe Convention on 'Laundering, search, seizure and confiscation of the proceeds of crime' that extended the scope to other predicated offences – besides drug trafficking – and kept a balance between criminal law and human rights.

Council Directive 91/308/EEC was complementary to the aforementioned initiatives in the EU and was influenced by the forty recommendations of the FATF. The directive obviously had an immediate effect on EC countries, but it also sought to extend its application to several European Free Trade Association countries (Gilmore, 1999). Member states were encouraged to extend the list of criminal activities that were associated with ML and more importantly, the directive emphasized that not only credit and financial institutions are avenues for ML, but also other professions. Member states were thus encouraged to 'include those professions

and undertakings whose activities are particularly likely to be used for money laundering purposes' (EU, 1991).[9]

Directive 2001/97/EC amended the directive of 1991. Here, EU legislation is extended to cover all organized crime besides drug trafficking, and the EU budget is additionally shielded from fraud or corruption (EU, 2001). Another item of focus in this directive is professional secrecy in conjunction with money laundering. For example, legal advice is left intact under the condition that the lawyer does not himself participate in ML, or the client does not ask for expert advice in order to carry out ML (ibid).

Directive on Prevention of the Use of the Financial System for the Purpose of Money Laundering, Including Terrorist Financing (Directive 2005/60/EC)

There is no doubt that the major shift of emphasis in this directive of the European Commission (also known as the 3rd Directive) involves the introduction of a risk-based approach. Dominance of the term 'risk-based approach', which includes a tremendous number of ambiguities, will be analysed in Chapter 6 of this book after both the theoretical treatise on systems theory is presented and the findings from the case study outlined. While this initiative has been amended in part by Directive 2008/20/EC, these changes are not considered significant enough to be discussed as a separate section here. If there are any implications stemming from these changes, they will be discussed within the scope of Chapter 6. Table 2.2 outlines the most important contributions of a few major AML initiatives.

AN OVERVIEW OF SOME GLOBAL AML FEATURES

It is useful, in closing the literature review and the broader review of the AML domain, to refer to some interesting facts that surround the global AML perspective. Some of these are of particular interest as they invoke some intricacies around the domain of AML, as well as the challenges that its community is facing.

Let us start by the observation that no member of the G7 has ever been blacklisted for whatever reason. This comes as no surprise as politics interfere with most groups, and the FATF has been no exception. Obviously, this does not mean that London, New York, or any other major city of a G7 member country are not heavily involved in money laundering. Most of the money being transmitted from major cities is tainted with cocaine (Lilley, 2000).

Table 2.2 The most important contributions of AML initiatives as they have evolved over time

Year	*Name of Initiative*	*Major contribution*
1988	United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (the Vienna Convention)	Required that all States recognize money laundering as a criminal offence, which also becomes extraditable. It is however, drug offence oriented.
1990	*Council of Europe on:* 'Laundering, search, seizure and confiscation of the proceeds of Crime'	Extended ML to other predicate offences. A State could prosecute even if the offence took place elsewhere and there was a careful consideration of third party involvement. Thus, the convention tried to strike a balance between criminal law and human rights.
1990	*Financial Action Task Force* The Forty Recommendations	FATF became the first group to focus solely on ML, and even though lacking in legal power, it set the 40 recommendations as a standard.
1991	European Economic Commission *– Council Directive 91/308/EEC*	Not only credit and financial institutions, but also other professions and categories of undertakings that may engage in activities likely to be used for ML, are taken into consideration. Thus, the scope broadens even more.
2000	United Nations Convention Against Transnational Organized Crime	ML is expanded to include all serious crimes besides drug-offences. The convention also expands the supervision to non-bank financial institutions.
2001	European Community *– Directive 2001/97/EC*	EU legislation embraces all organised crime under ML and not just drug-trafficking. Professional secrecy is also a focus and legal advice is left intact (unless the lawyer knows that ML takes place, or takes part).
2001	Financial Action Task Force *– Special Recommendations on Terrorist Financing*	Trying to frame terrorist financing as money laundering. Many however have objected to these recommendations as they argue that it is not ML but something that should be treated separately.

Table 2.2 (continued)

Year	*Name of Initiative*	*Major contribution*
2003	Financial Action Task Force – *Revised Forty Recommendations*	Various updates on recommendations and particularly a more abstract handling of typologies-based handling of AML.
2005	European Commission Directive 2005/60/EC	Considerable shift of emphasis affecting all stakeholders involved in AML by the introduction of a risk-based approach in treating the problem domain and mostly in prioritising over the submission of filing STRs to FIUs by considering the risk-based approach (for example as in the case of high-risk customers).

What is so special then about blacklisted countries? The Financial Action Task Force claims that blacklisted jurisdictions are those that have failed to put in place measures for carrying out AML effectively. But if that is the case, what could one make of the MI6 agent who literally destroyed a vital ML investigation (Rider, 2003), the affairs between the UK and its protectorates (Mohamed, 2002), or the fact that the Pentagon was actually selling biochemical equipment (via the Internet) that ended up mostly in the Middle East, all through a shell company and on a discount reaching 80 per cent of the purchase price (Demetis, 2004)?

The shocking story of the Pentagon selling biological and chemical equipment through the Internet was actually discovered by the US Congress. The latter had set up a fictitious company through which they bought (off the Pentagon) the equipment. Obviously, the contradiction between the fact that the US was (and is) fighting terrorism and the Pentagon selling equipment that could be bought by would-be-terrorists has sent shock waves across the US government. Interestingly enough, the story received minimal publicity. Furthermore, it seems that there was a clear policy in the US Department of Defence that prohibited any selling of items.

Similar inconsistencies become more evident in particular examples within the AML community. As a case in point, we can turn to the example of Nauru, the smallest republic in the world with a total land area of 21 sq km. It has refused cooperation after being blacklisted, and has also managed to launder around $70 billion in 1998 (Lilley, 2000). Nauru demonstrated to the world that geographical isolation has nothing to do with ML, especially when it is supported by a full Commonwealth

membership. Blacklisting from the FATF would follow (with a 2 year lag!) and even though it is generally perceived that blacklisting causes trouble for business (as countries face barriers whilst transacting with the world's largest economies and other AML community members), several jurisdictions have resisted the consequences for prolonged periods of time. Because of the nature of the ML phenomenon, money can be channelled and laundered in various ways.

Nauru was placed on the FATF blacklist in 2000, and in 2001 passed its AML Act. With a change of government in Nauru, 139 offshore banking licences were revoked (Johnson, 2003). As the AML Act failed to meet the obligations (according to the FATF), the OECD declared probable sanctions against Nauru and more than 18 countries required increased scrutiny in all transactions involving it (Roule and Salak, 2003). The US Department of Treasury also published proposed regulations to impose special measures against Nauru under section 311 of the USA Patriot Act (ibid). But if we consider that the reported number of countries that requested increased scrutiny in transactions involving Nauru and put this number in a global perspective, then that did not even come close to the membership size of the FATF, let alone the international community. Even though a number of stakeholders requested increased scrutiny for transactions involving Nauru, the country did not face particular difficulties in transacting with other markets. This is why three years after the problems were identified, the country was still holding a place in the blacklist up until 2004. Furthermore, in their effort to impose sanctions on Nauru, the United States tried to make use of the Patriot Act whereby financial institutions would be required to terminate the correspondent accounts with Nauruan financial institutions (ibid). But that (according to the Act) would include correspondent accounts maintained for other foreign banks that are used to provide banking services indirectly to Nauruan financial institutions. The feasibility of such impositions is questionable since it implies a high level of information sharing where even indirect transactions can be monitored.

This example may considerably put into question the very function of organizations like the FATF. Severe criticism has been levelled at how the FATF deals with countries that become blacklisted, and it is not clear with what criteria countries are being chosen for review, or what the audit procedures are. A well-respected expert in the field of AML, Peter Lilley, makes the following remarks:

> After February 2005 the blacklist was down to three countries, as the FATF removed the Cook Islands, Indonesia and the Philippines as each of these countries were 'implementing AML measures to remedy deficiencies that were

> identified by the FATF'. In October 2005 the list was reduced to its current 'rump' when Nauru got the green light to become respectable and was removed from the list after it had abolished its 400 shell banks which, in the words of the FATF 'removed the major money laundering risk'. Thus as at February 2006, only two countries – Myanmar and Nigeria – remain 'blacklisted'. Yet frequent references are made to other countries where weak or nonexistent AML controls exist. *Whilst the FATF exercise has clearly improved AML regulation in numerous countries has this process simultaneously (for whatever reason) allowed other jurisdictions to pass under the radar screen and carry on facilitating the washing of dirty money?* (Lilley, 2006)

One might perhaps offer a series of criticisms in these assertions, including the impossibility of effectively scrutinising and reviewing every single country, however, Lilley's point cannot go unnoticed: how much of the ML reality is being constructed by the agendas initiated by the FATF (and to a large degree being politically dictated) and how much of this FATF exercise allows other jurisdictions to go unnoticed? Even worse, how are financial institutions to tell what jurisdictions should be considered more 'risky' in ML and terrorist financing (TF), if the FATF offers no mechanism to help other than naming a limited number of countries?

In addition to this, it is interesting to note that – at the time of writing of this book – no countries whatsoever were being featured in FATF's infamous blacklist (also called the Non-Cooperative Countries and Territories list) while at the time of editing of the book in January 2010, only Iran, Uzbekistan, Turkmenistan, Pakistan, and São Tomé e Príncipe were featured in a statement issued by the FATF. That being the case, there is a pressing need to consider different approaches in dealing with this extremely important phenomenon within the realm of ML, and always in conjunction with the risk-based approach. Also, the analysis for such an endeavour would need to take into account not only the financial aspects of a region and the risks involved, but also political aspects and instability that may generate corruption. These conditions threaten the regional socio-political structures of a society and cultivate potential avenues for ML and TF (given that corruption, turmoil and socio-political risk create a perfect setting for such activities).

It is however inevitable that some institutions will see AML as an opportunity for expansion rather than a problem that needs to be solved. An example comes from the involvement of the IMF and the World Bank. Their respective executive boards, which wanted to proceed to a unified methodology (with the FATF), wondered what their ongoing relationship with the FATF should be, and further suggested that the latter should refrain from blacklisting until a consensus was reached (Holder, 2003). Of course, and despite considerable IMF efforts for expansion to the AML

domain, the FATF blacklisting process will not just cease to exist. It incorporates and personalizes both the role and the institutionalization of the FATF. It is one of its ontological constructs.

The functionalistic and hence prescriptive logic that is followed by the international community projects an overly simplistic picture of a very complex system, one that can supposedly be controlled by just 40 recommendations (plus eight more for terrorist financing to satisfy the modern appetite on the war against terror). This clearly demonstrates that despite the clear progress that has been made throughout recent years in strengthening efforts and the myriad of legislative initiatives, a truly international flavour against ML is still missing. It also demonstrates that what has been often termed as a 'holistic' approach for tackling AML is not only missing, but has also been barely researched. Even though the term 'holistic' induces grave observational misunderstandings (as we shall see), it does however hint towards treating the AML domain as a whole, or even better as a *system* in its own right.

If there is one major contribution that this book is claiming, it is that of dealing with AML through systems theory. It aims at providing systemic considerations and insights that surpass the purely descriptive levels that seem to have exhausted their possibilities, and rarely go beyond a mere pragmatic/typological based treatise. In other words, this book attempts to elaborate on systems theory as the theoretical framework that can be used to inform anti-money laundering research and practice. Even though this appears to be an academic endeavour that aims to provide a theoretical ground for research, there are considerable implications for practitioners. These implications emerge from within the chapter where the case study of a financial institution is discussed (Chapter 4) and also in the chapter dealing with the risk-based approach (Chapter 6). There are also considerable practical considerations in the utilization of various information systems for AML purposes. But before we go into an exposition of systems theory in the following chapter, it is best to discuss first the subject matter of anti-terrorist financing.

THE FARCE OF ANTI-TERRORIST FINANCING (ATF)

Ever since the FATF introduced the eight special recommendations on the financing of terrorism, a lot of energy has gone into dealing with this subject matter and the focus of the FATF has somewhat changed. Many stakeholders have expressed doubt over the feasibility of the endeavour of ATF and while tackling terrorist financing still remains on the agenda of

both regulators and practitioners, no research has discussed the current status quo of ATF and actually expose it for what it is: a farce.

It is at least in this author's contention that the fight against terrorist financing presents itself with a severe contradiction: a paradox. This paradox becomes visible under specific circumstances when stakeholders like financial institutions attempt to combat the phenomenon. One such particular instance is the automated manipulation of transactions by technological means to spot TF. Similarly to what is done for ML, the key concept of *profiling* is introduced and profiles are constructed that attempt to simulate the behaviour of someone who finances terrorism. But in the case of terrorist financing, things become considerably obscure. A series of questions beg answers. What is a profile for someone who finances terrorism? How much money is required for the financing of a terrorist attack? Does the word 'typology' even make sense in the case of TF without resorting to discriminatory practices that often touch upon sensitive issues of race and religion?

Beyond the simple requirement of testing for those suspicious persons that appear in the OFAC (Office of Foreign Assets Control) or CFSP (Common Foreign and Security Policy) lists, profiles need to be constructed and technologically embedded so that the activity of terrorist financing can be modelled. But how can someone construct a profile for a terrorist financer? The short answer is that it is extremely difficult to do so, simply because a wide number of elements increase the difficulty of the profiling process. Profiling terrorist financing (from the standpoint of financial institutions that are obliged to be vigilant and report unusual activity) has to be based upon the instrument that financial institutions have at their disposal and upon which they can apply the profiles; this instrument is no other than the totality of each institution's financial transactions. The problem here is that terrorist financing is a completely different process to money laundering and consequently both the methods of profiling and the manipulation of these methods require knowledge that cannot be applied to financial transactions. Secondly, the amount of money that is required to finance a terrorist attack varies greatly and cannot in general be compared to the vast sums of money being laundered. Other than the already existent OFAC and CFSP lists that prescribe suspicion for terrorist financers, all other attempts to profile TF on the basis of financial transactions resort to mere speculation.

Quite far from the deluded aspirations of some politicians, the involvement of financial institutions in this saga against terror has created considerable confusion, organizational and compliance problems. It is even tempting to say that the enterprise of automated profiling of the activity of TF appears to be a lost cause. To put it more mildly, a direct quote will be

used from the FATF guidance notes for the detection of TF by financial institutions. In that quote, the FATF mentions the following:

> It should be acknowledged as well that financial institutions will probably be unable to detect terrorist financing as such. Indeed, the only time that financial institutions might clearly identify terrorist financing as distinct from other criminal misuse of the financial system is when a known terrorist or terrorist organization has opened an account (FATF, 2002).

It becomes imperative that the obvious is stated here. If the FATF acknowledges that 'financial institutions will probably be unable to detect terrorist financing as such' within FATF's guidance notes for the detection of TF (hopefully one sees the irony here!) then what is the point altogether of troubling financial institutions with this task? Also, what is the possibility of a known terrorist or terrorist organization opening an account instead of having one of their non-listed associates do it for them or even better utilize a number of underground Hawala-type methods readily available for moving money around?

In their book, *Countering Terrorist Finance*, Tim Parkman and Gill Peeling indicate that 'those sums spent by active terrorist cells on the preparations for a conventional terrorist attack are typically so small as to be mere droplets in the ocean of daily financial transactions' (Parkman and Peeling, 2007). Then they move on to argue that 'what must not happen is that while everyone is focused on name checking and the impossibility of detecting 'suspicious' $500 ATM withdrawals, some multi-million dollar nuclear-related financing scheme passes through the system undetected' (ibid). The latter scenario that is presented as a possibility is indeed an alarming scenario (that of a nuclear-related financing scheme); but that is a possibility, which is almost impossible to prevent by scrutinizing financial transactions. Indeed, intelligence agencies are much better equipped to monitor attacks of that type and when necessary request – from financial institutions – the monitoring of specific individuals and their transactions. Confidential briefings of compliance officers by intelligence agencies have been used for that purpose in the past few years and these briefings appear to be much more fruitful than guidelines for monitoring TF and typological discussions that can hardly be integrated in any automated system without resulting in hundreds of thousands of false positives.

With more than 1400 terrorist organizations that have been (and most still are) in existence over the past 30 years, most terrorist incidents have required little funding while evidence for state-sponsored terrorism is scarce in most cases (and politically dictated). Even though the agenda for pushing terrorist financing along with money laundering has clearly been political, it is worth reflecting on some of the most recent and publicized

terrorist attacks. According to an enquiry by the BBC World Service that interviewed officials from the Scotland Yard and acquired information by experts on the financing of terrorism, the financing of the London underground attack 'cost only several hundred pounds' (BBC, 2006). Also, the Madrid train bombings are estimated to have cost $10 000 and the 9/11 attacks cost between $400 000 and $500 000 to execute (9/11 Commission, 2004). These figures make one wonder whether the mobilization of the global financial system is well worth the trouble when tackling terrorist financing is like looking for a needle in a haystack and when intelligence agencies remain underfunded in most countries. Another example may highlight this point further. On the basis of an analysis carried out on a database (access was acquired to that database through the library of the London School of Economics), it was found that more than 12 200 terrorist attacks were recorded in the past 30 years. Amongst those attacks, 169 different nationalities participated overall, a fact that demonstrates that there is considerable geographical spread over those who are involved in terrorism of some form (this of course depends on the definition of terrorism, another vague construct). In any event, this geographical spread is in stark contrast to what organizations and countries are targeted for TF. With OFAC blocked funds targeting just eight organizations, and with 98 per cent of all block funds corresponding to just two of the eight organizations (namely Al-Qaida and Hamas), a truly international effort against terrorist organizations is clearly non-existent. Such a perspective would require intelligence agencies to find better reaction-mechanisms, although these are bound to be politically controversial in the case of terrorism. The very fact that only $2648 has been confiscated for the financing of the Taliban according to the latest available Terrorist Assets Report (OFAC, 2007) makes a rather strong statement on how 'efficient' the fight against terrorist financing has become.

Regardless of the methods that will be advanced for the tackling of terrorist financing, it must be stressed that the problem of data growth presents an ever-greater information asymmetry in this case (Demetis, 2009). The volume of data that needs to be monitored when taking into consideration the low-value of transactions that are required for a terrorist attack to be financed, as well as the rate of occurrence of terrorist attacks (apparently much less frequent than ML), makes the monitoring of TF an undisputable thorn in the heart of any profiling method. But to the politicians that have initiated the regulatory pressure on this matter, this is all apparently non-consequential. It really does not matter if there is any shred of effectiveness in involving financial institutions in this fight against terror. High-level institutional endorsement of the subject matter of ATF and a constant repetition of its importance by a variety of sources,

stakeholders, and mass media, have indeed managed to convince us of the 'validity' of this absurdity. Meanwhile, intelligence agencies remain underfunded in most countries.

Even though it becomes evident (from the discussion in the previous sections) that the monitoring of TF is considerably more difficult than that of ML (GATE, 2008), it must be stressed that insofar as technology has influenced the monitoring of both problem domains, the interference between computer profiling and human profiling remains critical. Both ML and TF are influenced by technology in ways that have to do with the monitoring and profiling of these activities, but the fact that the huge volume of data that underpins such processes must be related to pragmatic responses in an organizational setting, elevates the theoretical problem to one of organization and technology.

3. On systems theory

INTRODUCTION

This chapter essentially constitutes a first step in presenting a coherent theoretical framework that can be applied to anti-money laundering research. Even though some key ideas are presented here, systems theoretical inferences and further theoretical development takes place in Chapter 5. This work is based on a number of research papers the author has published on the application of systems theory to the problem domain of AML (Angell and Demetis, 2005, Demetis and Angell, 2006, Demetis, 2009, Demetis and Angell, 2007). However, it is only in the scope of a book that the theoretical background can be laid down in more detail and the concepts surrounding systems theory further elaborated.

Anti-money laundering is a demanding research domain that is interdisciplinary in its core. As a research area, it draws researchers from a wide number of fields. Researchers that have a legal background examine the interferences and consequences of law on AML across various nations, as well as bilateral and multilateral treaties. Researchers that have a social sciences and/or economics background usually attempt to examine the provenances and effects of AML or draw its micro- and macro-economic implications. Researchers that come from the natural sciences (for example physics or mathematics) participate in the formulation of mathematical models that can be computationally integrated for the modelling of ML activities (that is profiling) or investigate – numerically – the size of the ML market through statistical analyses and mathematical modelling. But while it is apparent that AML draws a wide number of researchers from across different disciplines, communication between those researchers is severed by distinct approaches and differences in approaching the subject matter. Furthermore, it has gradually become evident that most research in the field of AML is rather descriptive, something that is reflected by the endless case-by-case ML presentations and the continuous typological examinations. While these typological examinations remain useful for practitioners, academic research ought to be grounded on a theoretical level and assist in drawing the implications for practice. A theoretical treatise on AML that could act as a platform for communication amongst

researchers of different disciplines is currently lacking and it is among the key purposes of this book to investigate this gap and provide a theory that can fulfil the promise of AML interdisciplinary research. This chapter takes a first step in describing the key theoretical ideas around systems theory. These key theoretical ideas are subsequently used to enhance the empirical data collected and presented in the case study in Chapter 4 and to expose a number of issues in Chapter 6 where the risk-based approach is analysed. The present chapter deals first with an introduction of systems theory and its importance within the broader theoretical domain (as well as its descriptive power). The concepts of difference and distinction are subsequently presented, followed by the key concepts of system, boundary and environment. There follow sections that deal first with the concept of complexity and then with self-reference, the latter being the key concept within the latest stage in the evolution of systems theory. Researchers interested in applying systems theory to the domain of AML will find in this chapter a variety of theoretical constructs that could assist them in conceptualizing distinct AML areas.

ABOUT SYSTEMS THEORY

Systems theory should be thought of as a collection of highly abstract concepts that can be applied to a series of problem domains. It should not be thought of as a single entity, a unity of a theoretical framework that is universally applicable. No previous theory has achieved such a feat, not that it would be possible to tell, as no system can accurately and fully describe itself, because the whole process would collapse to a form of paradox that would entail a tautology. The reason that no system can accurately describe itself is because asymmetry must be seen as a fundamental prerequisite for the construction of any system, an assertion that is theoretically justified further on. Furthermore, every theoretical formulation, every theoretical construct and application, becomes inextricably bound up with an *observer* (say a researcher) that is employing the concepts of the theory for her/his own purposes. Hence, theory construction, deconstruction, reconstruction, and application, become severely dependent on the observers who employ these operations and conceptual schemas for observing within particular circumstances and contexts.

Even though systems theory (ST hereinafter) has been in existence for decades, a series of paradigm shifts have occurred within the theory as is usually the case with any theory (Popper, 2002). These shifts have influenced the theoretical concepts themselves and have provided researchers with a number of descriptions that can be used in various problem areas.

A detailed examination of this theoretical evolution is an elaborate task and well outside the scope of this book, as one has to go back almost 400 years in the history of the influences behind ST. More than 35 major figures in the construction of the theory can be delineated; the theory itself has progressed from a mere mechanical model, to a biological model, to a process model, and then on to a different sphere that includes concepts like chaos, complexity, evolution and other important ideas (Bausch, 2002). These changes have contributed considerably to increasing the descriptive capacity of the theoretical constructs involved, something that has granted to ST the status of a grand theory. Whereas 'grand theories' appear to achieve the formulation of an all encompassing framework and attempt to explain a range of related phenomena with conceptual links between the constructs of the framework, 'little theories' provide a conceptual lens to view a particular set of situations without necessarily conceptually enriching links between concepts (Whitley, 2006). In other words, on one hand we have theories that can be characterized by a substantially abstract set of concepts (thus they can be applied to a wide range of problem areas because of the abstract nature of the concepts they engulf) and on the other hand we have theories that resemble well-defined frameworks (thus they can be applied to more specific circumstances).

If there is one thing that cannot be denied of ST, it is that it has achieved a considerable degree of maturity and its concepts have evolved to allow for the theory's implementation in a wide range of domains. But just what kind of systems can be studied with the help of systems theory? Answers present considerable variety as physical, biological, political, legal, economic, and even social systems (with the latter considered to be the latest step in the ladder of this theoretical evolution) have all been described through the use of the lexicon of ST, and the term grand theory therefore implies just that. Instead of ad hoc applications to a limited number of fields or frameworks that become applicable only within particular settings, ST is highly abstract and can be applied to a wide range of different domains. This is particularly the case for financial systems and the economic functions that they seek to fulfil. Many have suggested that the general conceptual framework of systems theory is clearly the strength behind the variety of implementations (Christin, 1983) and that extending systems theoretical concepts to practice is very important. There are also reasons that support the systemic approach towards managing organizations (for example financial institutions), as the assumptions that organizations are simple and 'closed' systems (and that the environment within which they operate is stable) no longer holds true. Organizations are 'complex open systems that are deeply influenced by and influencing their environments where . . . actions can give outcomes, which are unexpected and opposite

to those intended' (Glass, 1996). The aforementioned assertion appears to be highly relevant to the area of AML, particularly when we consider it as a complex open system, deeply influenced by its environment.

ST therefore studies systems of many kinds and such a diaspora into different disciplines means that systems theory is fulfilling its initial promise (Bausch, 2002). This means that there exists a portfolio of multi-disciplinary applications of the theory, and so ST would seem ideal for adoption in the fields of information systems and AML, fields that are truly interdisciplinary. Particularly for information systems, ST could also help establish an identity for the field, which has faced considerable crisis as to whether it even constitutes a distinct discipline (Avgerou, 2000). Indeed, prominent scholars in the field of information systems (IS) have not refrained from suggesting that systems theory could bring out the full potential in information systems research by providing both rigour and relevance, as well as by providing considerable new insights in the socio-technical sphere and within interpretivist research (Lee, 2003). At the same time, we ought to recognize that ST has already contributed considerably to the field of IS (Xu, 2000). In an era of increasing complexity in the implementation and implications of information systems (for example on problem domains like AML), the systems approach has even more to offer in the conceptualization of any problem domain and the extent to which that domain is influenced by technology (ibid). Contemporary phenomena that challenge the way we view the integration of technology within society require such theoretical tools for their examination (Kallinikos, 2005a, 2005b, 2006).

ST must be seen as a set of highly abstract concept-tools that, if used appropriately, can potentially give considerable insights into the complexities of a system that is to be examined, a system like AML. The fact that there are many who argue that the lack of success of ST is its very generality and that it does not allow for the development of methodological solutions (Lin, 1988), does not appear to be convincing at all. In fact, viewed systemically this would be a contradiction within systems theory, which dismisses cause-and-effect relations. A decision to act on a problem domain can only trigger changes with undetermined consequences, and these in their own turn can become the basis for even more decisions, and so on. Solutions always 'multiply, proliferate, disperse, circulate, diversify, diffuse the original problem' (Rossbach, 1993). This is true for the system of society itself, which within the scope of its own self-observation is able to stimulate itself; it generates 'problems', which require 'solutions', which generate 'problems' which require 'solutions' (Luhmann, 2000). Cause-and-effect merely implies a focal point, and that can only exist within the scope of either a single observer prescribing a solitary function for a

system (that if fulfilled will give the appearance that the duality between cause-and-effect is closely intertwined) or many observers with predetermined shared beliefs in cause-and-effect. But it is not only the belief that solutions cannot be attained with ST that appears to be troubling as a criticism. Far more disturbing is the underlying epistemic chimera behind cause-and-effect that is widely neglected and rarely confronted.

This major criticism against ST is therefore one that is inconsistent even within the logic of those who prescribe the lack of a suggested solution to be problematic. For if they criticize ST by employing a rational-logical mindset they neglect the fact (in their own logic) that if a problem uniquely prescribed its solution, it would cease to be a problem as it would immediately evoke its one and only (dis)solution (ibid). This latter assertion creates a different discourse on the whole enterprise of problematization, which must not be taken lightly. To think of ST as something like mechanics, which provides answers to problems with the answer built-in in the form of particular laws that govern the behaviour of systems is a grave mistake (Arbib and Cornelis, 1981). Equally it is argued in this book that it is fallacious to think of the environment of a system as a causal texture (Trist and Emery, 2000). ST is far more flexible, and allows for the specification of a few dominant assumptions about a particular system. The implications of these original dominant assumptions can be followed through or these assumptions can be altered in order to see what the changes imply (ibid).

ST, therefore, is considerably detached from any cause-and-effect relationships that often undermine and decontextualize the importance of the observer. Instead, ST tries to describe the problem domain as viewed by an observer, and ultimately describe the significance and interdependencies of complex processes within the system. In this manner, considerable insights can be gained by using the theory, but most importantly, increased vigilance can be achieved by looking into the systemic complications and implications that are entailed in decision-making processes (at any observer-level, such as regulatory initiatives), whether they involve technology or not.

No doubt, part of the reason that ST faces considerable criticism of the type outlined above is because it steers clear from reductionism, the practice of breaking up a problem into its parts and examining the parts instead (Crotty, 1998). ST diverges from such an approach, by examining the system as a whole,[1] something that does not mean that the parts of the system are not important. On the contrary, examination of the parts' interaction remains crucial in a systemic fashion. Also, additional emphasis within systems theory is given to the idea of *emergence*,[2,3] which will be further analysed in the following sections superseding the main

descriptions and review of systems theoretical concepts. It may initially appear contradictory how ST may stray away from reductionism once a system is defined as being constituted by subsystems, however, this is a restricted view of 'system'. There are considerable alternatives that complement such a structural perspective. In theoretical frameworks that are closely intertwined with a particular reference (or research) domain, theories have to adapt in order to accommodate new phenomena and/or incorporate changes from previous descriptions. The reason ST has endured is because, as a meta-discipline, it can be applied in a variety of domains where it successfully addresses problems 'beyond conventional reductionistic boundaries' (Skyttner, 1998).

DIFFERENCE AND DISTINCTION

According to Professor Niklas Luhmann, the key ST theoretician that this book draws its ideas from, we do not begin with an epistemological doubt and therefore we have to accept that systems exist. The fact that this is first and foremost a matter of observation makes it ever more crucial, as once one accepts this initial premise then it becomes crucial to identify the 'difference' that is to be utilized for further exploration and analysis.

The start point of any systems theoretical analysis is the difference between the *system* and its *environment.* Before proceeding with a description of the two distinct and different ways of 'viewing and decomposing' a system, it is crucial to conceptualize this *difference* between the system and its environment, and come to a realization that without the difference itself, the definition of any system would be impossible. The very process of defining a system has two subsequent and intertwined consequences: the creation of an *environment* that establishes this difference, and a delimitation that restricts the system's conceptualization by setting its *boundary*. This becomes more evident in the following paragraphs.

Indeed, there is nothing more difficult than to conceive of something in splendid isolation; that is, to imagine a system without an environment. The reason is simple; nothing exists in a vacuum! Far from being a trivial assertion, this is a foundational statement, because every observation requires a differentiation from something that cannot be observed. By defining a system, a conceptual boundary is unavoidably set; for without the boundary, the system would have been impossible to start with. Boundaries then cannot be conceived without something beyond and thus their very existence presupposes the reality of a beyond and the possibility of transcendence (Luhmann, 1995). Once the boundary is decided upon, the environment follows next. Even though the overall *triality*[4] (system,

boundary, and environment) is automatically created as soon as any act of observation takes place, it is intriguing to note how the human mind naturally constructs the concept of the system first and proceeds further with conceptualizing the rest.

Of course, this process does little to restrict alternative descriptions, because one can always define a system otherwise, by defining the environment as the system, and so on. Still, a testament to this process of differentiation comes with the recognition that the theoretical construct itself is a 'systems theory', not a 'boundary' or 'environment' theory. Even if we define the *triality* as another system, all we have done is to introduce a meta-system, which is itself another system with a boundary and an environment, ad infinitum. This daunting infinite regression (that progresses in the sense alluded to by Nietzsche[5]) in the construction (or even deconstruction) of systems should not pose a problem.

The definition of a system, indeed any definition for that matter, is above all an act of choice and an observer-relative act. The observer is crucial in the construction of any system, as the construct implies the application of a *distinction* or a *difference*. ST has the capacity of describing itself in this manner; systems theory therefore sees itself (and any other scientific theory) as a contingent distinction, a distinction that could have been drawn differently (Luhmann, 1998). But regardless of such a difference in the drawing of the distinction for what constitutes a system, the difference between system/environment must be seen as absolutely fundamental.

It is truly impossible to think of an example where the above is not the case; that is to think of a system for which an environment does not exist. The most common fallacy is the *universe*. Even attempts to encapsulate the entire astronomical cosmos in a single word (universe) cannot abolish the idea of the boundary and its environment (Angell and Demetis, 2005). Physicists have been debating this issue for decades, albeit unsuccessfully, whilst trying to resolve the paradox of the expansion of a 'universe' into 'nothingness'. But apart from the physical or philosophical difficulties of this paradox, a consideration of the construct alone exposes the problem. What is the word 'universe', or any other word for that matter? Nothing more and nothing less than an element within a broader construct, with the overall construct being a notational schema like many others (Goodman, 1976), and a system in itself. In this example, whereby the notational schema is language within which the word 'universe' resides, we have to recognize immediately that 'language use itself is the choice of a system that leaves something unsaid' (Luhmann, 2002), particularly when words need to be interrelated for the production of meaning as, they too, cannot exist in isolation.

No system can therefore exist without an environment, because this is

the only way that a system can ever be defined. The process of distinguishing between system/environment is called *systemic differentiation*, and is crucial to the system itself, because a system can only have self-reference (that is, refer to itself), by differentiating between itself and an environment (Luhmann, 1995). According to Luhmann,

> Systems are oriented by their environment not just occasionally and adaptively, but structurally, and they cannot exist without an environment! They constitute and maintain themselves by creating and maintaining a difference from their environment, and they use their boundaries to regulate this difference. Without difference from an environment, there would not even be self-reference, because difference is the functional premise of self-referential operations. In this sense, boundary maintenance is system maintenance (ibid).

The difference between system and environment, a prerequisite for the self-reference of any system, has considerable implications for the act of observation, and hence for research itself. What we observe then ultimately conforms to a distinction, and without the distinction there would be no observation. In one of his theoretical masterpieces entitled 'Theories of Distinction', Professor Luhmann points out:

> When observers (we, at the moment) continue to look for an ultimate reality, a concluding formula, a final identity, they will find the paradox. Such a paradox is not simply a logical contradiction (*A is non-A*) but a foundational statement: The world is observable *because* it is unobservable. Nothing can be observed (not even the 'nothing') without drawing a distinction. . .or to say it in Derrida's style, the condition of its possibility is its impossibility (Luhmann, 2002).

As the above assertions about the construction of both system and environment indicate, the environment should not be seen as something residual to the system (Luhmann, 1995) but as something that is constitutive of the system's existence. As the book moves on to discuss the concepts of the system, boundary and environment, the aforementioned comments should be kept in mind.

THE SYSTEM

There are two important ways in which we can describe just what a system is. It is important to note here that any systemic description and observation must conform to the fundamental axiom of *distinction* that is constitutive of observation. In other words, in order to 'see what is inside' a system, that is in order to decompose the system itself, we will have to form yet another distinction. Typically, such a distinction is manifested

in the two following ways: a) a system is composed of subsystems, b) a system is composed of elements and relations.

Each of these scenarios is examined separately and in order. If we state that a system is composed of subsystems then the operational difference between system and subsystem does not become immediately apparent. This is because each subsystem can be defined as a system in itself and therefore distinguishing between systems and subsystems is a distinction that collapses automatically. What is then the guiding difference that can be used while decomposing a system into its subsystems? Where is the crucial differentiation here that allows for the observation to take place?

The answer to this question is once again, the difference between system and environment. The system replicates or mimics the difference between system/environment internally, and hence creates esoteric (internal) system/environment relations within it. Even though images oversimplify the issue, it is still useful to use one at this stage that could potentially help in conceptualizing this matter.

There are two unit-differences here that need to be considered. This means that the difference is essentially one (between system/environment)

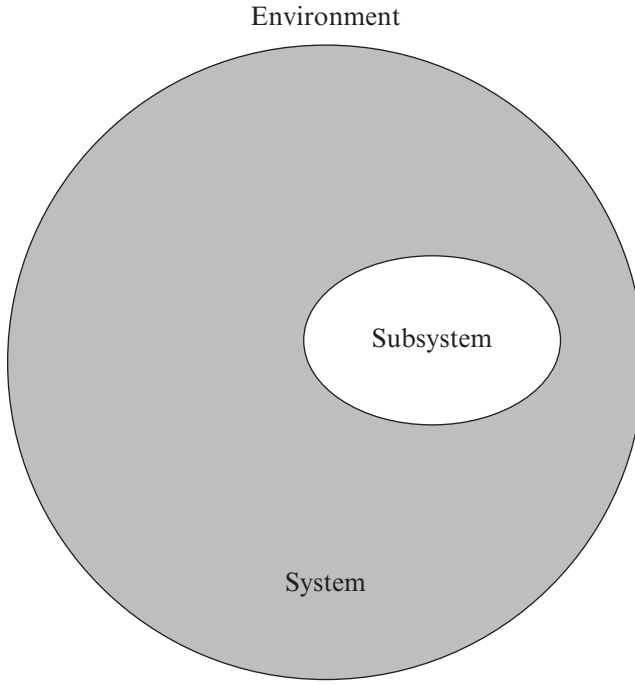

Figure 3.1 System/environment distinction

and that this difference exists simultaneously at two different levels as it is internally replicated in the system. The system in this scenario is the circle (which clearly incorporates everything in it, including the subsystem) and is differentiated from its environment. However, the system/environment difference is replicated internally. For the subsystem therefore, the environment is the internal sketched area within the system. An interesting point emerges here that remains to be solved: is the external environment (external to the system) also an environment for the subsystem? Even though this is counterintuitive in many ways, the answer that is guided by differentiation would be no. But what would then be the difference between the two differences? In other words, what is the difference between system/environment (externally) and system/environment (internally)? One must realize here that first and foremost this is a matter of observation, and that the definition of the system guides this process as it is only in this scenario where system/environment esoteric differences can be realized. The difference in internal (or esoteric as Luhmann calls them) system/environment relations is that they enjoy inferior complexity when compared to the exoteric system/environment difference; this is because the mechanisms for investigating internal complexity are highly structured, observed by the system itself, and accessible in the communicative processes during the formation of the system. The difference between the two differences can therefore only make sense a posteriori of the definition, observation and constitution of the system. Without the definition of a system, both esoteric and exoteric system/environment differences would have been impossible. But even more so, esoteric system/environment differences can only be realized once the entire system is taken for granted.

The decomposition of a system into its subsystems is, however, a clearly structural perspective. Systems are composed of subsystems; subsystems are composed of sub-subsystems, ad infinitum. The system itself is seen as an assembly of components that are organized as a whole (Checkland, 1985) while each component works autonomously for a specific goal (Zemke, 2001). In this process, it is not really these complexes of components that make a difference; their interaction is far more important (Bertalanffy, 1969). Even though the statement that a system is composed of subsystems might look like reductionism, such an assertion is fundamentally flawed for a series of reasons, the foremost of which being that it neglects the issue of *emergence.* Whereas reductionism is the process of breaking up a problem into its parts and studying the parts instead, systems theory primarily deals with emergent phenomena and the complexity that generates them.

Having discussed the first aspect of viewing the decomposition of a system, we now turn to the second scenario whereby a system can be

defined by its elements and their relations. This difference is crucial. As there can be no system without an environment, elements cannot exist without relational connections (and vice-versa). These two distinct possibilities of viewing the decomposition of a system underpin different aspects of systems theory, both of which are equally important and complement each other considerably. The first kind of decomposition (system/environment) refers to *system differentiation*, whereas the second kind of decomposition leads to *system complexity* (Luhmann, 1995). This distinction is crucial because:

> Only this distinction makes it meaningful and nontautological to say that system complexity increases with an increase in differentiation or with a change in the form of differentiation. Elements can be counted and the number of possible mathematical relations among them can be determined on the basis of their number. The enumeration reduces the relations among the elements to a quantitative expression, however. The elements acquire quality only insofar as they are viewed relationally, and thus, refer to one another (ibid).

This quote from Professor Luhmann requires special mention, as it lies at the very core of how systems theory deals with the relations between elements. To illustrate this critical point that is found in many different types of systems, the example of the human brain[6] is used. If one poses the question 'can one cell think?' then it becomes obvious that the answer is in the negative. If however one starts enumerating the cells in the human brain that are close to 100 billion, it becomes obvious that put together they construct a system of a different order, a function-system that produces cognition (Coward, 2005).

The argument here must be made loud and clear. There comes a point where, by putting things together, a change occurs which is not solely quantitative but one that is denoted by a considerable *qualitative* shift. The whole is more than the sum of its parts, a concept dating back to Aristotle. This renders reductionism irrelevant for describing higher-level systemic formation as for any system like the brain, decomposition into its structural parts fails to describe the new laws that govern the new levels. Such new levels experience what are utterly emergent phenomena; these depend upon the connections created amongst different elements within the system. An ever more crucial question, and one that merits considerable pondering (even though one can barely provide any conclusive comments in this regard) is how the threshold is being determined within the system whereby this change from quantitative to qualitative occurs. How many cells does it take to start thinking? How is that determined in the system as it evolves?

Such difficult questions and their pondering should be left aside as what

determines the emergent behaviour (in any system), or the undetermined consequences, is heavily dependent on the system itself. Far more important is the recognition that there are indeed *emergent phenomena*, a set of properties that are based on, yet emerging from the system's components and their interrelations (Germana, 2001); such emergent phenomena cannot be predetermined. They cannot be expected. One can therefore speak only of emergence as a phenomenon itself; a phenomenon that is based upon the internal complexity of a system and a phenomenon that comes into being without being preconditioned by any one observer.

THE BOUNDARY, THE ENVIRONMENT ET AL

Following the definition of the system, we now turn to the importance of both the boundary and the environment, and associate them with the concept of the system itself. Through the exposition of the boundary and the environment, other important aspects and systems concepts will be unveiled.

As already discussed, no system can exist without a boundary and without an environment. There is however a fundamental difference between system and environment. For each system 'the environment is more complex than the system itself, as systems lack the requisite variety (Ashby's Law) that would enable them to react to every state of the environment, that is to say, to establish an environment exactly suited to the system' (Luhmann, 1995). It is an unavoidable fact therefore that the system is inferior in complexity to its environment, and so has to compensate for such inferiority by 'exploiting its contingency, that is, by its pattern of selections' (ibid).

The Law of Requisite Variety is crucial in conceptualizing this difference between system and environment, and hence requires further analysis. Suppose that we have two entities named R and D respectively. Both are participating in a strategy game. For example, we can pick R to be the system, and D to be the environment. What Ashby posits is captured in the following sequence of inferences: if R's move is unvarying, then this means that R carries out the same move over and over again. Subsequently, D's move would not matter because *the variety in the outcomes would be as large as the variety in D's moves.* In such a scenario, D would be exerting full control over the outcomes. If however, R had two moves, then the variety of the outcomes could be reduced to a half (but not less).

An important issue here is that only the variety in R's moves can force down the variety in the outcomes. Put differently, only the system's variety can force down the variety in the environment. As Ashby frames it: 'Only

variety in R can force down the variety due to D; Only variety can destroy variety' (Ashby, 1958).

This means that if the system is to survive the changing environment, then variety and flexibility must be introduced and enhanced. At this point, another problem emerges that requires further clarification. If the environment (for any system) is far more complex than the system itself, then how is it possible for the system to survive at all? Doesn't the variety in the environment, which enjoys superior complexity (to the system), destroy the variety of the system, and ultimately the system itself?

Two crucial aspects resolve this matter. One has already been mentioned, and refers to the system's contingency. The system exploits its contingency, and therefore it can develop strategies for stabilizing the difference between itself and the environment; however, it is only the system and not the environment that can develop strategies for stabilizing this difference (Luhmann, 1995). The way the system exercises and stabilizes this difference can now become clearer, and lead us towards another concept; that of the boundary. But before we proceed to describing the boundary and its vital importance, there is one more aspect that is related to the system's variety, and the reason why environmental complexity per se cannot force the system to immediate collapse. The environment itself is an agglomeration of different systems, and these conform again to the same principle of system differentiation. They too have an environment with no immediate access to its complexity. Hence, any system, both within and outside of any specific observer-defined system itself, has a complexity that is characteristic of its variety; such variety is limited as it is strongly related to the process of systemic formation when the system was constituted and came into being. If that weren't the case, then there would be no co-evolution between any system and its respective environment. There would be no systems at all, as they would immediately collapse from their environmental complexity, and the very act of observation would restrict itself to instantaneous flashes of systemic formations and destructions.

Needless to say, experience says otherwise. Not only do systems exist, but also they maintain their existence by 'controlling' their boundary and appear to be relatively stable in a constantly changing world. System and environment engage in a structural coupling, a form of co-evolution; structural coupling means that there is an interaction between the system and its environment, but it does not mean that the evolving structure of the latter can causally determine the changes in the former. The environment acts as a trigger for the subsequent structural changes that occur within the system (Maturana and Varela, 1998). This means that the entities in the environment and their actions, once they are perceived by the system, may initiate changes in the system. But the opposite may also

happen. Structural changes in the system also affect the environment. One of the reasons that no causal relations can be found in the process of structural coupling is because both system and environment are constituted by a great number of stakeholders (systems in themselves), something that renders the monitoring of all interactions impossible (Angell and Demetis, 2005).

Clearly, it becomes evident from the aforementioned comments that the boundary has a distinctive role to play in any systemic formation. However, defining the boundary is no easy task, as it is ambiguous by its very nature. The boundary is simultaneously part of both the system and the environment. Hence, strictly speaking, there can be no causal control over the boundary for any defined system and for its respective environment. Complexity and variety within any difference between system and environment imply a continuous struggle because of the feedback between them. The fact that there can be no control over the boundary can then be complemented with the description that systems can increase their sensitivity to boundary feedback through self-organization and improved communication amongst their subsystems. Thus, systems appear to be able to 'control' their interaction with the environment but without any cause-and-effect mechanisms whatsoever. Even if the system increases its sensitivity concerning boundary feedback, and hence tries to 'control' the boundary, there is no way to predict environmental responses.

What then is the purpose of the boundary? What is its importance? Clearly, to answer these questions in-depth we will have to resort to the boundary's ambiguous ontological status, and the fact that the boundary is at the same time both part of the system and the environment. It is this property of the boundary that essentially establishes the difference between system and environment, makes the differentiation between the two possible in the first place, and mediates the interactions between them. Put differently, the purpose and function of the boundary is to allow for the exchange of *feedback* between the system and its environment. As feedback is an interactive process, this means that changes in the environment will feedback across the boundary to modify the system itself. Furthermore, changes in the system will feedback across the boundary to modify the environment. Feedback in this sense becomes vital for the structural coupling between the system and the environment, and feedback essentially constitutes the exchange of codified information being transmitted between system and environment. From the system's perspective, this feedback can take two distinct forms, namely *positive* and *negative* feedback.

Positive feedback affects the system in a way that ultimately threatens the system's existence. Within positive feedback lie the seeds of chaos

that may explode systemic stability and amplify the processes that carry the system away from its reference state thus leading to disorder. A reference state in this regard is recognition of a temporary state of the system that is used to monitor minor variations. An initial marginal event can, through positive feedback, be the cause of long term dramatic events of the Lorenz butterfly effect, named because even the 'insignificant' flapping of a butterfly's wings, through complex feedback, can trigger a major weather feature (Hilborn, 1994). Due to the butterfly effect in any system, modelling and prediction becomes impossible; we have to accept the unavoidable fact that in a non-linear world the future is open and uncertain (Ramos-Martin, 2003).

Each system is constantly fighting for its own survival. Positive feedback may reach a point of flux, creating havoc among the subsystems and the processes they use to communicate, which can lead to the break-up of the system. Sometimes, the break-up can trigger the reform and regrouping of the subsystems as a new system, or it can lead to extinction, especially in cases where there is little unity of purpose among the subsystems. Another outcome is a slow process of receiving positive systemic feedback that might give the impression of a relative stability – albeit transitory – but it still leads to an increase in entropy. Obviously, all possible outcomes cannot be accounted for because of the complexity. The actual outcome depends on what subsystems will survive the forceful processes that occur within the system, and how they will change it. Subsystems may also be rendered obsolete from changes in the environment. One thing is certain. What we term as a system is neither a stable nor an unambiguous entity.

Negative feedback on the other hand has a clear opposite role and meaning from that of positive feedback, and that is to counteract any disruptive processes in order to reinforce the relative stability of the system (Angell and Smithson, 1991). Both positive and negative feedback are most closely related to the concepts of entropy and negentropy respectively. Whereas entropy leads to the disorder and death of a system, negentropy is the exact opposite (relative stability). All systems tend to be entropic with the maximum state of entropy being death, and the apparent contradiction that arises when pondering the question of the possibility of systems being negentropic can be quickly resolved once we look towards the environment. So how is it even possible for systems to be negentropic? Since every species on the planet exploits the resources of the environment in order to be negentropic in the short-term (Mayr, 2000), so systems can exploit the resources of their respective environments for the same purpose.[7]

Such a systemic exploitation of environmental resources (no matter how one defines the system) is considerably supported by the capacity and

capability of the system to probe the environment through mechanisms of information exchange. The process of probing is made considerably easier as both system and environment are characterized by a property that does not allow them the flexibility of cause-and-effect exchanges, but instead introduces risk, uncertainty, and emergence; that property is complexity.

COMPLEXITY

Complexity is regarded as a systemic property, specific aspects of which will be incorporated into this chapter without examining the truly vast setting of complexity theory; this is because the inner workings and evolution of complexity theory are complex in themselves, display no characteristics whatsoever that could approach a unified theory, and contain many different branches of research (Mitleton-Kelly, 2003). For the purposes of this book, and as complexity will be used to describe particular systemic instances, a few crucial points will be described that will be absolutely fundamental when reflecting upon the concept of complexity and its consequences; for complexity is not a methodology, but a way of thinking (ibid); such a way of thinking has been used extensively in systems theory as an important property of systems.

But why is there such a thing as complexity? There are several reasons that point towards acknowledging its existence. One of the most important reasons establishes complexity via the impossibility to monitor all the interactions that take place within a system at any given time. Such impossibility is based upon observation itself, which operates through a (series of) distinction(s) and hence creates the possibility for unobservable interactions. This important role and function, which complexity preserves within systems, makes it no accident that the concept of complexity has been applied in several fields like biology, physics, mathematics and computing, and that the literature surrounding complexity has exploded in the recent years (Maguire and McKelvey, 1999). However, despite such an explosion in the literature on complexity, relatively little work has been done on complex social systems (Mitleton-Kelly, 2003), with the notable exception of Luhmann and a few others (ibid), and even less so on complex systems that include technologically oriented processes and the extent to which technology influences the complexity of those systems.

For money laundering (*not* anti-money laundering here), complexity is absolutely fundamental, as it is a generated prerequisite for concealing transactions and blurring the money trail. Therefore, in ML we stumble upon a different type of complexity that is propelling and exploiting the intrinsic patterns of systemic complexity. In such a scenario, complexity

becomes an absolutely critical mode of functioning for the money laundering system itself, instead of something that needs to be avoided or reduced. The AML system therefore faces a type of complexity that is deliberately generated by those engaged in ML, all the while dealing with its own systemic complexity. Within such a setting, technology becomes crucial, as complex technology-based processes supporting AML create a series of systemic phenomena requiring considerable research (Demetis and Angell, 2006). For these reasons, and since delving into the too many different aspects and variations of complexity research is outside of the scope of this book, it is still necessary to include a small section on complexity in this chapter as it is interwoven and interrelated with ST, and can enhance the analysis that follows after the presentation of the research findings. Meanwhile some comments hopefully clarify some of the ambiguity in concepts that are interrelated with complexity.

Chaos and emergence are two such concepts that are confused with complexity. One of the most common misconceptions is that chaos and complexity are fabricated in a way that formulates a proportional co-evolution (in the fashion whereby complexity may even equate to chaos). But it is not just chaos in the complexity (Gleick, 1988). Spontaneous order and stability can also appear, however the complexity of the interaction of elements in a system cannot, on its own, explain the behaviour, or predict the coming into existence of any emergent properties (Angell and Demetis, 2005). Emergent properties are simplifications among the complexity (ibid), and the possibility always remains that the same order of complexity can spawn different emergent properties. Emergence is therefore simply one of the characteristics of complexity, while others include self-organization, connectivity, feedback, co-evolution and so on.

In a previous section, mention was made of fundamentally different ways of viewing the decomposition of a system. One such way pointed towards the system/environment differentiation, and the other the difference between elements and relations that leads to systemic complexity. Within the scope of the latter difference between elements and relations, elements matter only if they are viewed relationally within the system. When it comes to systemic complexity as a phenomenon of emergent elemental complexity this has an important complication that essentially describes the process of systemic formation or constitution. According to Luhmann:

> We will call an interconnected collection of elements 'complex' when, because of immanent constraints in the elements connective capacity, it is no longer possible at any moment to connect every element with every other element. In this respect, *complexity is a self-conditioning state of affairs: the fact that elements must already be constituted as complex* in order to function as a unity for higher

> levels of system formation limits their connective capacity and thus reproduces complexity as an unavoidable condition on every higher level of system formation. *We may hint at the fact that this self-reference of complexity is then 'internalized' as the self-reference of systems* (Luhmann, 1995).

Hence the most crucial observation that one can make regarding the importance of complexity lies within the scope of a system's constitution and formation. Elements within a system cannot but be characterized by restrictions in their connective capacity, for without such restrictions (that are being posed by higher level systems), elements would not be able to function as a unity.[8] Complexity viewed this way is something that cannot be avoided, but it is a property that is necessary and without which higher-level systemic formations would be impossible; elements can only be viewed as participating in the complexity when the overall system emerges and at the same time the participation of elements becomes dependent on them compromising their own internal complexity in order to interconnect with every other element. This reveals a very crucial point: interconnections between elements imply a compromise without which the interconnection would not have been possible to start with. Complexity then becomes an emergent property in systemic formation, a necessary compromise for the elements that need to interconnect, and one that limits their intrinsic capacity to do so.

This incompleteness in the connective capacity of elements is extremely crucial and aligned with the fact that observation implies the differentiation between what can be observed, and what cannot; a differentiation that is crucial for it is only by not-observing that one can observe. This then implies that 'the observer points towards an incomplete selection, whose incompleteness is made necessary by the fact that comprehension of world complexity must be coordinated with the possibilities of its reduction' (Rossbach, 1993). Following observation, comprehension of world (or environmental) complexity, and the necessity for the reduction of complexity, creates then the concept of systems as *'islands' of reduced complexity* (Luhmann, 2004). If systems are portrayed as islands of reduced complexity then they exist within an environment of high complexity (ibid).

Here we reach another key point: observation implies delimitation, a focus on what can be observed, and by doing so, guides the process of reducing world complexity. Complexity in this regard means 'being forced to select; being forced to select means contingency; and contingency means risk' (Luhmann, 1990, 1995). Even more importantly, the mechanism by which a system reduces world complexity is guiding itself internally in the selection of its elements, as well as its elemental interconnections

and communications; the mechanism for reducing world complexity is self-reference. More will be said later concerning the relationship between complexity, risk, and communication.

SELF-REFERENCE

Continuing on from the description of complexity, which has a central role to play in a system's properties and, as discussed earlier, occupies a role constitutive and interrelated in systemic formation, it is time to discuss a key concept within ST, the concept of self-reference.

The fact that self-reference has a key role to play in theoretical descriptions becomes evident from the concept's use in major philosophical and scientific works. In a truly insightful comparison of the works of Michel Foucault, Friedrich Nietzsche, and Niklas Luhmann, author Stephen Rossbach describes how Foucault came close to the concept, Nietzsche even closer, but it was only Luhmann that made self-reference the centrepiece of his work. According to Rossbach, Luhmann managed to retain concepts of systemic complexity for constructing a theory for social systems, but also managed to consolidate systems theory (Rossbach, 1993).

However, Luhmann himself didn't just invent the concept of self-reference. He was greatly influenced by the entire enterprise of cybernetics (for example Ashby, 1958) and in particular, second-order cybernetics (Bateson, 1972, Korzybski, 1948, Von Foerster, 1951, Von Foerster and Josiah Macy Jr. Foundation., 1950, Von Foerster et al., 1962) that already included concepts of control and communication, learning and adaptation, evolution, and most closely, *self-organization* (Scott, 2004). With the theory's use in biology, and in particular via the concept of autopoiesis (Maturana and Varela, 1998), other changes soon occurred and more distinctions were elaborated: autopoiesis is one such example. Autopoiesis as a concept describes systems that have the capacity to 'make themselves'; systems are constituted with the ability to refer to themselves and their constitutive elements, thereby reconstituting their functioning parts. This presented a most notable and crucial connection in biology where Maturana and Varela made the connection with the idea of self-organization.

One of the first accounts of the concept of self-reference comes from Korzybski in describing language as a 'uniquely circular structure, where an "effect" becomes a causative factor for future effects, influencing them in a manner particularly subtle, variable, flexible, and of an endless number of possibilities' (Korzybski 1948). Over the years this idea of a structure that is uniquely circular has intrigued the many

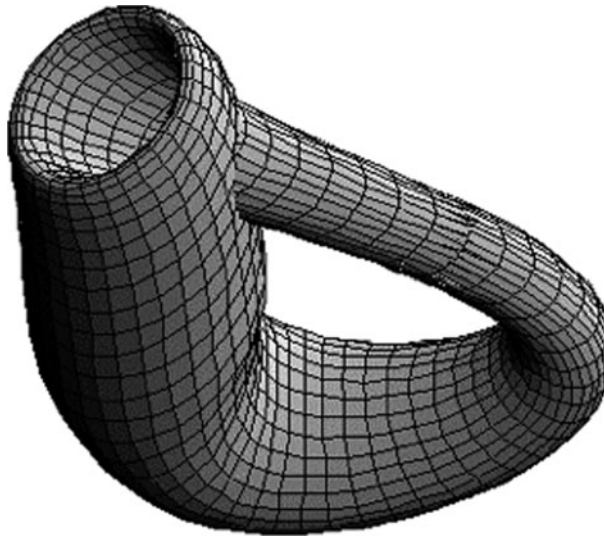

Figure 3.2 Mathematical self-reference and the representation of the Klein bottle

researchers that attempted to describe a bizarre form of re-entry, a form that enters itself and hence can be characterized as self-referential. Many have attempted visualizations of this form of re-entry through mathematical descriptions of the constructs, and one of the most successful visualizations describing re-entry has been reconstructed above, that of the Klein Bottle.[9]

The relationship between complexity and self-reference is also very crucial, and it is no accident that the major ideas around self-reference are presented here, following the section on complexity. For if the system, any type of system, perceives an increase in environmental complexity, such an increase can only be made manageable via a series of self-referential processes that have the potential to increase the system's internal complexity, and hence the pattern of selections within the system. These in their turn can allow for a greater degree of flexibility and responses from the system, although such a process cannot be characterized by any causal mechanism. In this manner, self-reference can also be recognized as the crucial mechanism with which the system reduces environmental complexity.

The literature predominantly distinguishes three meanings for the concept of self-reference. According to Felix Geyer, these are: a 'neutral' meaning whereby any changes that occur in the system's state are dependent

upon the state of that system at a previous moment; a 'biological' meaning whereby the system contains information and knowledge about itself; and, the 'stronger' second-order cybernetics meaning whereby a system collects information about its own functioning, which in turn can further contribute to a change of its functioning (Geyer, 2002). Some requirements for the latter to occur include self-observation, self-reflection, and some flexibility in acting for decision making (ibid).

This book acknowledges the major influence of the latter description of self-reference, one that comes very close to Luhmann's use of the term. The description given also comes close to the organizational and technological implications for AML that will be further discussed.

With these initial comments, it must be made clear that self-reference implies more than a mere reference of the system to itself. If that were the case then this would simply end up in a tautological form that would be of little or no use and one that would be completely de-contextualized from the broader systems theoretical context. Self-reference must instead be seen as a central concept for the system, which can now be delineated as follows:

1. Self-reference as fundamental for systemic formation and systemic survival. The system refers to itself and its constitutive elements, but also maintains that (self)-reference for sustaining its processes and their outcomes (these refer to processes of learning and giving meaning). In this way, the system is autopoietic, for otherwise the system collapses if self-reference is not maintained.
2. Self-reference as fundamental for reducing environmental complexity. The system refers to itself and the relations that support it, so that it can exploit its *pattern of selections*, and hence either increase its internal complexity and contingency, or refer to processes that can utilize streams of such contingencies and that could potentially handle the environmental changes. Utilization of such streams of contingencies are often reflected in the system's subsystems.
3. Self-reference as fundamental for information processing, whereby the system refers to itself and the abstractions within itself, in order to perform computations supported by information and communication technologies.

This last aspect of self-reference put forward here has direct implications for the two former aspects. It implies that technology constitutes a system and is partly detached from organizational processes to form a distinct technological realm (something that will be further supported through the case study). Nevertheless, the term *system* here needs to be further

clarified, as in no way does it imply a mere technological installation, a common confusion.

Technology as a system has systemic effects, is characterized by an internal complexity and is utilized to respond to environmental complexity. Technology is equipped with all the systemic properties discussed thus far. But even more importantly, technology as a self-referential system affects the way in which various interrelated aspects of information processing are handled within its domain. This description of technology as a self-referential system is used in order to discuss some absolutely crucial and fundamental perspectives on technologies used in AML, like profiling and data mining. Such technologies have come to influence the realm of AML considerably through the electronic processing of information that they facilitate. While they support an information exchange both between system/environment as well as between elements/relations within the system, they are also constantly being probed for changes via they organizational processes they support.

The term *system* is therefore assigned a completely new meaning; that of self-reference. Such an example comes from the field of socio-technical studies where we can consider an information system as what emerges from the interactions between a technical system and a social system (nowadays this understanding is engrained within the minds of IS researchers). This does not however imply that neither *technical system* nor *social system* are self-referential, and that only the emergent system enjoys self-referentiality. Quite the contrary; just as technology – at a macro level – is used to produce other technology in various forms (a self-referential process in itself), and just as a social system reproduces itself, so too does an information system. We must not forget that the definition of a particular system, or any definition for that matter, is observer-relative. But once a system has been identified and observed, self-reference becomes unavoidable. Without self-reference, the system would not have the capacity to refer to itself and its function. That however would lead to a paradox as the observer has a priori identified something to be a system and ultimately the power resides with the observer that decides upon the distinctions he/she employs.

As Luhmann claims, we do not start with epistemological doubt; systems exist and insofar as they exist, they are self-referential. However, before continuing it must be thoroughly understood that according to the tradition of systems theory, what in common parlance has come to be termed *system* has absolutely nothing to do with the term *technical system* used here. Indeed, even most people within the IS community refer to the word system when all they mean is the installation of a technical system; one that is instantiated as a technological artifact (or series or networks of

the latter). Typical of such a stance is the simple observation that within 'systems analysis and design', the term 'system' refers merely to the installation of the technical system, something which is symptomatic of the lack of a systems approach in the IS field.

Still, as argued in previous paragraphs, self-reference can be found at any systemic level. Through the introduction of self-reference at the level of information processing, an example is offered here that may resolve the technological implications of self-reference.

The example concerns a pattern recognition algorithm.[10] Imagine that a human being has handwritten on paper a large number of single digits (say 1000 digits ranging from 0 to 9). These digits are then scanned and used as an input to a computer system that is supposed to determine what is the actual number that the human being has written. A computer algorithm is therefore called upon in order to determine what each handwritten digit actually corresponds to. The basic principle that is used here is that the shape of each of the ten digits is different and hence by having a set of abstract characteristics for identifying individual digits (for example shape, curvature of lines, and so on), the algorithm should be able to differentiate between an 8 and a 9 or between any given numbers. As one might expect, this works well most of the time, but it does also often stray away from expectations. Here enters the notion of probability. The computer can then estimate what is *the probability that a handwritten digit corresponds to the identified number*. The better the match between *a handwritten digit* and the *abstract set of characteristics that define that digit computationally*, the higher the probability that the digit matches with the identified number. If one were to represent these probabilities, one would rightly expect a variation in their scattering due to digit mismatches, higher or lower probabilities of correct matches.

What matters in this example is not how efficient the algorithm is in identifying digits correctly but the distinctions employed in the abstract process for carrying out the identification. Through this example, two crucial and different concepts must be discussed regarding pattern matching, an equivalent term to profiling. These concepts are *categorization* and *abstraction*. A category represents many entities within it that we may call instances of the category. While the instances display a notable variation within the category, the category in itself has to be related to an abstraction through which the category is represented. Let us take the digit '2' as an example in order to examine this matter. This conceptual delineation would take the following form: the *instances* would refer to all individual images of the handwritten number two, the *category* would be the collection of all such images of the number two, and the *abstraction* to which the category is attached would be the number two itself.

Categorization then takes place in two distinct stages, one involving the conceptual delimitation of the category (that is the definition of the category), and another the algorithmic representation of the category and its computational processing. Let us examine these two stages in somewhat more detail.

In the scope of the first stage, someone has to designate what categories are to be considered. In this particular example, every number (0. . .9) constitutes a category. A particular category is then examined more closely, say the one that constitutes the collection of all such images of the number '2'.

The function that technology comes to fulfil within this process of categorization is to act as an automated means of deciding the category where each individual image can be assigned (as previously noted). But in order to do that, from a computational standpoint, the algorithm that carries out the task of this internal decision-making process requires a mechanism for the decision to be made. This mechanism, which determines how the algorithm operates, is then based upon the juxtaposition between an *abstraction* and a *specificity.* The algorithm in effect constitutes the set of rules that penetrates this distinction between abstraction and specificity. The algorithm therefore examines how an *instance* (say any number from 0. . .9 according to the predefined categories) *fits the abstraction of every category*.

Within this process, however, an important problem emerges as there is a considerable variation within the examined instances. For example, there are multiple instances of the handwritten number 2 that have to be categorized by the algorithm. But that does not mean that the categorization carried by the algorithm will be effective. A badly handwritten 2 can be misrecognized as a 3 and so forth. Beyond these trivial technicalities, the important thing to consider is that all these underlying technological processes are manifested by reference to an abstraction. *Abstraction then becomes the schema for information processing within computation.*

How the abstraction relates to the concept of self-reference may not be immediately visible, but essentially, self-reference within this context becomes the underlying structure for information processing. Technology refers to the constructed abstraction within itself in order to carry out what is labelled as 'information processing'. The abstraction is then deconstructed with the purpose of determining the abstraction's elements that may be used. If the purpose of the comparison within computation is pattern matching, then the deconstruction of informational elements from the abstraction will involve shape, curvature of lines, and a series of other such attributes that will be searched for against incoming instances. The attributes will play the role of simulating the abstraction, but the

entire computational process will have to accept a foundational error on the premise that *the abstraction is unique while the actual incoming instances are multiple*. From this difference, a set of problems emerges almost spontaneously and the process is jeopardized in effectiveness within several computational stages and interactions. The most important of these are:

1. The representation of abstraction has to be deconstructed and this causes difficulties with incoming instances; deconstruction essentially determines what is a 2 in pattern matching according to the computation. Since different values may be given to analyse the ideal curvature of lines of the number 2 in its shape and so on, this implies that the abstraction of the number 2 that is computationally deconstructed can have a variety of representations.
2. For the example of pattern matching, the incoming instances have to be recognized as numbers (0s, 1s, 2s, . . .9s) and hence a suitable deviation has to be accepted as a basis of error. An incoming handwritten instance may not be an ideal number 2 according to the attributes extracted from the abstraction, but if its attributes exhibit 'similarities' within *accepted deviations* then it is accepted as a 2.
3. The construction of the categories is arbitrary and how these categories (or their interaction) come to affect the output, a potential evaluation, or other computational processes remains prone to the initial determination of the categories.

If the example did not involve pattern matching digits, but instead simulating money laundering behaviour, then the underlying computational process would exhibit the same foundational properties. In a ML example, a *model* replaces the abstraction of a number with properties describing what constitutes money laundering behaviour. The categories are replaced by queries that have certain attributes describing money laundering on the basis of transactions (frequency, time of association of the customer to the financial institution, age, location, amount). Finally, the instances within the categories (in the former example these were the variations of a category, such as all handwritten digits of the number 2) are replaced by individual financial transactions. Such financial transactions are therefore screened on the basis of categories and their representational abstractions. All this is done in the hope that suspicious transactions will eventually be produced. Not by human beings but by technology.

When the comparison is made between the two examples (pattern-matching and money laundering behaviour) the conclusion is inescapable. One can imagine a similar kind of variation in probability but this time

concerning an effectiveness index of spotting suspicion for ML. Successful identification of ML cases is even more greatly compromised by the complexity of the ML problem domain and the wide variety of informational elements that have to be considered.

Regardless of the problem domain, when it comes to technology, the system refers to itself in comparing what it receives as data *against* its systemically imposed abstract schemas. This process continues as long as the system is utilized and hence all information processing becomes self-referential.

The above example points towards a crucial aspect in self-reference that should be emphasized: self-reference has nothing to do with tautology; it implies systemic differentiation at its very core. The asymmetries that are created between *abstraction and category* and/or *category and its elements* remain a fundamental prerequisite for self-reference; otherwise the system would have been incapable of internally differentiating between the abstraction and the constructed categories. In this regard, the distinction between internal input and external input becomes elusive, irrelevant, and utterly decontextualised in the scope of information processing and self-reference. What occurs is simple: external input is internalized within the system, otherwise the processing cannot take place.[11]

Later in this book (following the description of the case study) further discussion and examples will probe and examine this underlying systemic core of information processing, to highlight underlying deficiencies in all technical systems that claim to target money laundering. Such deficiencies are systemic and intrinsic to the technical systems employed, and the manner in which such systems come to affect each other.

Self-reference however should not be merely associated with such elemental information processing. Self-reference is what characterizes any system identified by an observer. The technical system clearly has a distinctive role to play within any other system that utilizes information processing, and therefore it becomes particularly relevant for financial institutions that are major users of computer technology.

4. The case study of Drosia bank

INTRODUCTION

This chapter discusses the main findings from a case study that was carried out over a three-year period in a financial institution in the EU area. A confidentiality agreement between the author and the financial institution cannot allow for an in-depth analysis of the context within which it operates so that the identity of the institution is not exposed. The name of the financial institution and the names of any information systems that could identify the financial institution have been altered.

The findings from this case study present an analysis of the internal reporting system of the bank, the increase in the number of suspicious transaction reports and investigate the influences of various information systems on AML. In order to structure the presentation of the findings better, the AML system of the bank is primarily analysed by utilizing the following distinction:

1. Investigations into money laundering that are initiated by a request from the national Financial Intelligence Unit or a public prosecutor
2. Investigations into money laundering that are initiated by the bank's network of branches.

Along the aforementioned lines, critical information systems that influence anti-money laundering work are discussed. These include (among others) a Case Management System (CMS) where data is stored for all ML investigations, an information system that is used to identify customers uniquely and a profiling software that attempts to capture suspicious transactions.

ACCESS TO THE BANK

Before beginning to describe the main findings of this case study, the author would like to express his gratitude to all the staff members of the bank for their support, cooperation, patience, assistance and helpful remarks. As

already mentioned, confidentiality agreements do not allow the exposing of either the names of employees or the name of the bank being researched; these obligations are honoured throughout this chapter.

First of all, the name of the institution has been changed to that of *Drosia bank*. The author was allowed access to the following:

1. The Know Your Customer policy
2. The policy on money laundering
3. The internal regulation of the bank concerning the monitoring of unusual transactions
4. Suspicious transaction reports initiated from staff members across the branch network of the bank
5. Reports that the Money Laundering Reporting Officer (MLRO) forwards to the national FIU
6. Access to the Case Management System (CMS) of the bank where all cases concerning money laundering are recorded
7. Statistical data concerning the whole branch network of the bank and the reports filed from each individual branch
8. The entire manual of the Case Management System as provided by the company that was responsible for its development (the project of building the CMS was outsourced)
9. The bank's intranet containing all the internal guidelines
10. The POSEIDON information system which contains basic account information for the customers of the bank, and is used by the money laundering analysis team
11. The specification requirements for the CHIMERA online system, a system that is used for the profiling of suspicious transactions
12. The Fast Transmission of Electronic Messages (FTEM) System, a system that is used to facilitate communication between the Compliance Group and all the branch offices of the bank
13. The Electronic Updates System (EUS), which is used to inform tellers and other personnel by electronic means
14. The CRONUS online system where banks share information between them
15. Online training material
16. The ZEUS system for the automated profiling of money laundering.

Besides documents and access to these systems, a series of semi-structured interviews were conducted with various stakeholders from Drosia bank over the three-year period. These include series of in-depth interviews with: the money laundering reporting officer of the bank (MLRO), the money laundering analysis team (MLAT) that is responsible

for the manual scrutiny of suspicious transactions, the manager, the assistant manager and other personnel working in the MLAT, the compliance group and the information systems analysis, design and management team of the bank. Stakeholders from a number of other institutions were interviewed as well. These include the national banking association, the central bank, the ministry of finance and the FIU.

The largest number of both semi-structured and unstructured interviews was conducted with the MLAT of the bank, the unit within the bank responsible for receiving the suspicious transaction reports from the bank's branches and subsequently undertaking investigations before deciding whether a report is suspicious enough for the MLRO to approve it being sent to the FIU. Also, the MLAT alone has access to the Case Management System for recording suspicious transactions for money laundering cases.

GENERAL COMMENTS ABOUT THE BANK

While it is very difficult to describe a bank without exposing its identity, some broader comments can be attempted. Such comments aim at an overview of the anti-money laundering processes within the bank and the steps that have been taken thus far towards improving AML. These will briefly precede the more extensive discussion on the suspicious transaction reporting system of the bank, the increasing number of suspicious transaction reports and its effects, the working processes underpinning AML, and the role of information systems therein.

Drosia bank is a major financial institution in the EU region. It has swiftly reacted to improving its internal procedures and working processes for AML from the very first introduction of the national legislative initiatives concerning money laundering. Two important related policies were introduced, one on Know Your Customer (KYC) rules and another on money laundering. The KYC policy of the bank clearly outlined the objectives of having such a policy in a short consolidated guide that was distributed to all the employees of the bank. Emphasis was given to several issues, such as customer identification, suspicious conduct and suspicious transactions. The policy also outlined the importance of such identification every time a customer relationship is established with the bank, as well as stressing the collection of sufficient information for the development of individual transaction profiles for customers. Even though what information should be collected for the development of transaction profiles was not clearly stated in the KYC policy of the bank (with the exception of a few examples like age, occupation and location), the intention of

collecting such data indicated a shift towards an automated profiling of transactions. An outline of how the process of identification should take place is clearly stated within the policy. It covers personal accounts, other deposit accounts and correspondent accounts. Ways of identifying a customer's true identity are discussed and increased vigilance is suggested on the various occasions when the origin of funds might not be clear. Money laundering typologies are discussed and consolidated with practical advice for the bank's tellers, as it is they that constitute the first line of defence against money laundering activity (an assumption that does not, for the moment, consider the issue of electronic banking). Consideration of the aforementioned aspects also takes into account data protection legislation, so that the processes behind any information gathering, storing or processing is in line with national articles of data protection.

The policy on money laundering extends that of KYC, and emphasizes the risks associated with money laundering. The bank's personnel are encouraged to do everything within their power to avoid involvement with any kind of illegal activity no matter how financially attractive the relationship with a customer might be. The broader outline of the money laundering policy places much emphasis on the protection of the bank, by putting issues like the preservation of credibility and reputation against possible abuse by money launderers. The policy on ML emphasizes the importance of KYC, thoroughly prescribes the process of reporting suspicious activities within the bank, and discusses the regulatory obligations that must be taken under consideration. Furthermore, the policy on ML addresses fundamental issues surrounding AML and discusses what day-to-day operations require protection from potential abuse by money launderers.

Increased vigilance on money laundering, the introduction of AML procedures, policies and guidelines within the bank, and the training of personnel have brought about significant changes in the reporting of suspicious transactions. As demonstrated in Figure 4.1, throughout a ten-year period between the years 2000 and 2009, the bank has seen an important increase in the number of STRs that were submitted to the money laundering analysis team by the bank's branches.

In order to accommodate for such a change in the volume of suspicious transaction reports, the bank has taken a number of steps to train and employ even more staff within the money laundering analysis team. For this trend in the increasing number of STRs, experienced by most financial institutions worldwide, the MLRO made the following comment:

> Such an increase is indeed alarming but nevertheless expected. The ongoing training of personnel is one of the reasons behind this trend and we are likely to

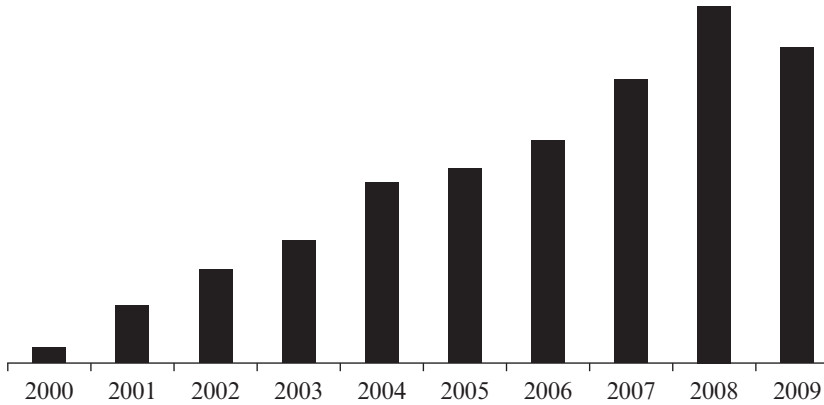

Figure 4.1 Increase in the number of STRs

> expect even more STRs in the years to come for multiple reasons (i.e. legislation changes, new information systems in the bank, etc.). We have already requested additional resources to handle such an increase and we are likely to employ even more people to handle it. AML however is only a cost centre within the bank so that might create a few frictions when asking for more resources.

Such an increase has become the source of a variety of problems in terms of investigation, and has brought subtle issues to the surface on what it would mean to be efficient within the internal reporting mechanisms of the bank. In particular, despite the fact that the number of STRs had increased considerably within this ten year period, the percentage of reports that were deemed suspicious and worthy of reporting to the FIU became gradually disproportionate to the increase in STRs. Therefore, as the number of STRs increased, the percentage of STRs that were submitted to the FIU tended to decline!

Figure 4.2 deserves particular attention. In the year 2000, nearly 73 per cent of the STRs received from staff reports were forwarded to the FIU after investigation from the MLAT. That number reached the peak of 84 per cent in the year 2001, while in the year 2004 the percentage of STRs that were forwarded to the FIU had dropped to 28 per cent. Between 2005 and 2009, that percentage was around 35 per cent on average.

Following this finding and a series of discussions concerning Figure 4.2, the following observations and comments were made:

1. According to the manager of the MLAT, the number of reports sent to the FIU in the first two years (2000, 2001) does not reflect the quality of the reports sent to them. Fear-compliance along with potential

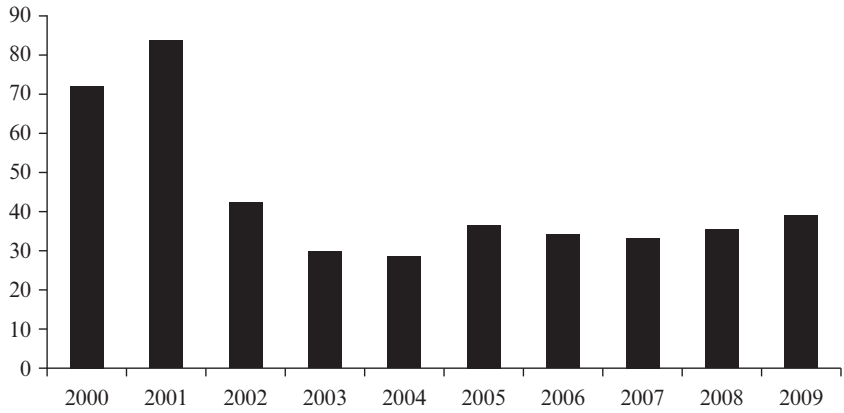

Figure 4.2 Percentage of reporting to the FIU

fines from the supervisory authority also played a role in such a high percentage of reports being sent to the FIU.

2. The sudden drop in the reports sent to the FIU between 2001 and 2002 (84 per cent and 43 per cent respectively) reflects a change in senior management and a new line of action. The MLAT was encouraged to be more cautious, to refrain from excessive reporting and to focus on those cases where serious suspicion for money laundering existed. Complementary to this change in the internal policy of the bank, it is worth noting that the FIU had also contacted the bank informally and urged it to submit fewer STRs as the volume of reports from the totality of the banking system was clogging the processing capacities of the FIU, and was creating a severe backlog.
3. Despite the increase in STRs suggested from Figure 4.1, throughout the last two years, it is worth considering that such an increase has done little to affect the percentage of reports forwarded to the FIU. This percentage has remained roughly the same from the year 2003 onwards.

Even though a full explanation for such relative stability cannot be pursued, there is an underlying qualitative aspect that underpins such a condition. That aspect is of systemic nature and associated primarily with a system's modes for processing information. Once a system reaches a certain degree of organization, then the internal quality that characterizes its information processing capacities does not usually deviate much from the norm. This may of course be easily destabilized by the introduction of technology, change in processes and so on. This having being said, a

more detailed analysis on such systemic implications can be found in the following chapter.

AML WITHIN THE BANK

There are predominantly two mechanisms that influence the work of the money laundering analysis team of the bank, namely: a) investigations on money laundering that start with a request from the FIU or a public prosecutor, b) investigations on money laundering that are initiated by the network of branches of the bank via the traditional route of filing an STR. In addition to those, we have the effects of the ZEUS profiling software that deals with the automated simulation of ML, but a description of these effects will be dealt with later on.

For the moment, let us turn our attention in the two scenarios described above. In examining the two, the role of Information Systems (IS) will become more evident in the broader suspicious transactions reporting system, while the ultimate purpose of the examination remains to expose that role and to examine the intricacies of particular IS implementations that have influenced, and continue to influence, the AML domain. The problems that usually emerge at a systemic level, an analysis of which is provided in the following chapter, come from the interaction of computer-automated systems and human-activity systems. The existence of such hybrid systems becomes extremely important in the understanding of the systemic effects of AML-related technologies.

An initial differentiation amongst these two mechanisms related to the reporting system will assist us in unfolding the details of the case study. This initial delineation is done between the two scenarios, each of which is analysed in more detail below.

EXAMINING SCENARIO A) EXTERNAL REQUESTS

Quite often, the national Financial Intelligence Unit or a prosecutor will request information from Drosia bank on investigations concerning ML. Such requests typically require the provision of raw transaction data from the bank. Sometimes these requests are limited to transaction data for a period of five years, and on various occasions that have become more and more frequent, the requests will require *all transaction data from the time of opening of the account*. It is worth noting that there are occasions when the FIU or a prosecutor requests all transaction data from the time of opening of the account irrespective of the size of the transactions. This

creates a massive explosion in the bureaucracy and the amount of documentation that has to be collected and forwarded to either the FIU or the prosecutor.

Such requests for the provision of transaction data by the authorities are handled by the Money Laundering Analysis Team and then forwarded appropriately within the bank. The first source of retrieving such data is the *Automated Centre for Transaction Recording* of the bank, which restricts itself to providing complete transaction records for the latest 40 months of the account's transactions.

With such a restriction posed by the Automated Centre for Transaction Recording, the bank makes use of an information system that was bought a few years ago, namely the Fast Transmission of Electronic Messages (FTEM) system. This system allows communication by electronic means, and interconnects all the branches of the bank with a centralized platform to which the MLAT has access. An employee from the MLAT will then gain access to the FTEM system, and manually input the information concerning the names being investigated. This becomes a considerable effort in cases where many names are being investigated and a number of details are required for each individual. From the point of view of the FIU this becomes even more problematic as different financial institutions require different identification documents. This was a problem that several financial institutions were facing as due to the lack of homogeneity in identification measures, competition was unfair and customers were inclined to prefer some institutions rather than others. Lack of homogeneity also exists in requesting identification documents for the opening of a bank account between the primary and the secondary holder. These difficulties were eventually ameliorated following an initiative from the banking association.

Once an employee of the MLAT records all the details of the names under investigation, an electronic message is sent via the FTEM system to all the branches of the bank. Individual branches must then process that information through their own link to the FTEM system. Access to the FTEM is gained by either the manager of the branch or the chief teller; they will typically check for such a transmission every two or three hours each day.

If it is found that any of the people under investigation have an account with a particular branch, the manager of that branch will assign an employee to investigate the physical records (transaction slips). Depending on the data that have initially been requested by the FIU, the employee will undertake the following tasks depending on the circumstances of the request: if the transaction data requested conform to a time period where the data are available in transaction slips, the employee will collect all the

slips and manually handwrite all the transactions on a pre-formatted paper form that is provided for this purpose. In the event that transaction data are requested from the time of the opening of the account, the employee will have to resort to microfilms where this data resides. Checking the microfilms for such individual transactions then becomes a painstaking process for the employees involved and might take weeks. The format of the microfilms is such that they are practically unreadable, and this renders the whole process of extracting transactions from individual accounts even more difficult. It is once again reminded here that these processes take place when all the transactions are required from the opening of the bank account and when they cannot be retrieved electronically in their totality. The reader here might automatically assume that technology would assist in this matter, and to some extent perhaps it would. But as we shall see, the complex interactions created by different information systems, create a series of problems for AML working practices.

In any event, once this cumbersome process reaches an end, it becomes evident how time-consuming AML investigations can become, especially if there is more than one branch involved in the collection of the transaction datasets. Once all the branches that have accounts under the names being investigated respond to the MLAT, the transaction records will be forwarded to the FIU for further examination.

The end result therefore consists of a folder containing printed transactions from the Automated Centre for Transaction Records along with all the remaining transactions that have been handwritten by the employees. On various occasions, the transaction slips have been requested as well. The National FIU or the prosecutors will therefore receive a printout of such information, as there are no facilities to allow for the electronic communication between banks and the FIU, and of course, such information collection is contingent upon the internal working processes and systems of individual financial institutions.

As shocking as the manual processes supporting part of the organized bureaucracy may appear, it should not be assumed that the capacity for a bank to submit all this information electronically would do anything to enhance the effectiveness of the national AML system. The experience from a number of countries where the electronic submission of STRs has been implemented (for example the United Kingdom) demonstrates that the burden is simply passed on to the FIU who has to find ways to filter the really suspicious transactions from the white noise. A similar situation is experienced when FIUs request raw transaction data to be sent electronically.

The FIU uses similar methods of communication with every regulated financial institution, so it becomes evident that data collection can be

extremely time-consuming. As those under investigation may have more than one bank account and often operate in different financial institutions, data-collection significantly increases the complexity of the investigation. The process of data collection alone can sometimes take three to four months before the data are eventually forwarded to the FIU for further investigation, and even then it is not clear that further data may not arrive at a later date from another regulated financial institution.

The FIU subsequently relies on a manual examination of such transaction data before forwarding to the prosecutor. Taken that the FIU employs a limited number of people, it becomes clear that a thorough investigation of all transactions is rendered difficult just by the volume of the documents collected. Furthermore, as no means of electronic processing is involved at this end, there is no mechanism for identifying if potential launderers involved in past investigations are named in the new reports sent to the FIU, unless someone actually remembers the name of the person being mentioned in past reports or if the suspect constitutes a primary suspect in a case that would have been filed under his/her name. For persons not identified as primary suspects in an investigation but for whom connections are established with those that are suspected of money laundering, there is minimal chance of detection and further investigation.

Those requests from the FIU or prosecutors targeted towards Drosia bank (or other financial institutions) that aim to retrieve all transactions irrespective of the scale of transaction, appear to be indiscriminate and demonstrate lack of understanding of the problem domain. Not surprisingly then, financial institutions like Drosia bank that have to undertake the task of data collection and have a better understanding of the internal working processes of their respective institutions, will often discuss with the prosecutors or the FIU, so that a threshold amount can be agreed before proceeding into data collection. For example, in an investigation that took place in the year 2007, there were so many transactions involved that it would be impossible and would greatly burden the authorities if the bank were to send all data irrespective of amount of transaction. This was discussed and it was finally agreed that only those transactions that were above €1000 would be forwarded.

EXAMINING SCENARIO B) INTERNAL INITIATION OF REPORTING

The second distinct way in which an investigation concerning money laundering takes place is when a member of staff from one of the branches of Drosia bank files a suspicious transaction report. That is done manually

through a standard form that the bank uses, based on the guidelines issued from the central bank. These guidelines make use of typologies that include amount thresholds. It has to be made clear, however, that whilst typologies are used when filing an STR, a transaction does not necessarily have to conform to any of those typologies in order to be reported. A narrative section is also found in the standard form, the importance of which has been stressed by all interviewees from the MLAT. In the narrative section, the employee that files the suspicious transaction report usually describes the reasons of reporting along with additional information that can be useful in the investigative part of the work. One of the problems of having such a manual internal suspicious transaction reporting system is that it is actually the bank tellers that have to fill out the reports, while at the same time these people have to serve the customers and barely have time for anything else. Staff members that further analysed these reports have often complained that the quality of handwriting is so bad that they can hardly make any sense of the content. The issue of internal electronic reporting as an antithesis to manual or hybrid systems will be dealt with in the following chapter.

The analysis of such manual STRs is undertaken by the Money Laundering Analysis Team (MLAT) and each one is assigned to a member of staff by the MLAT manager and investigated thoroughly before a decision is made as to whether the report deserves further consideration, attention from the MLRO, and potential forwarding to the FIU.

Every single STR that is received from the bank's network is logged on an information system that is a rather basic Case Management System (CMS) and a simple facility that the software provides is used to extract statistical information from the reports being investigated. Reporting statistical information from the bank to the supervisory authority (that is the central bank) is compulsory and takes place annually.

The CMS was installed in 1999 when most financial institutions started showing increased vigilance over anti-money laundering and sought after information and communication technologies that would facilitate parts of AML work. Ever since, it would probably be fair to say, the CMS system has become the main companion for work of the MLAT within the bank. Even when new STRs find their way into the MLAT, the team would first check whether there has been a previous report on the names being investigated within the CMS.

This particular software was bespoke and not an off-the-shelf solution. The project was outsourced to a company that undertook the task of building the software after working together with the personnel of the bank. The consultation period between MLAT and the company in charge of the project for building the CMS lasted for about two months with

only a few rounds of consultations. After the requirements specifications were formulated, the software was developed and installed. However, the company that took charge of developing and installing the software seemed to lack essential understanding of the dynamic nature of money laundering investigations (or the financial institution did not communicate them properly). This resulted in the creation of a software package with few capabilities, stringent processes and inflexible controls. Unfortunately, requirements specification was carried out hastily, and in a manner that prevented critical changes from being performed in the future, as they could potentially jeopardise the underlying informational infrastructure of the Case Management System that was already in place. This will be discussed to a larger extent later.

Far from being an automated tool that monitors electronic transactions and far from being a profiling tool for modelling ML behaviour, the CMS software operates offline with no link to any other system or database. As the manager of the MLAT commented:

> The software does not have any intelligence built into it. Actually it is not provided for that reason. It is very simple and in many ways restricts the work that we want to do. There are many instances where the software is inflexible. For example, if one bank branch merges with another, there is no way of putting those two together in the system. Therefore, subsequent non-existent branches will virtually continue to exist and cases on money laundering cannot be transferred to the branch that has taken over that information. Statistical information can only be extracted for particular categories while particular changes that we requested from the software company were not feasible for technical purposes. In a sense, we are locked into this particular platform which we have been using for nearly a decade now.

The manager of the MLAT continued on a quite different topic regarding the software, and in particular commented upon the fact that the particular software platform was operating offline:

> Sometimes it becomes evident that we are in many ways cut-off from live systems and unavoidably remain restricted into carrying out a post-mortem of the cases. Considering however systems that would automatically make such decisions on what is suspicious and what not (perhaps with some real-time intervention) might present other considerable difficulties.

Various other problems were discussed about the CMS. For instance, every case under investigation is input into the CMS with a unique reference number. However, subsequent investigations about the same suspicious persons would have to be inserted into the CMS with a different unique number, and according to the manager of the MLAT, this increased the

complexity of manipulating individual cases, and compromised the usability of the software in investigations. Apart from the CMS itself, there is however another information system that is being used by the MLAT, and which has played an important role within the bank itself.

THE POSEIDON INFORMATION SYSTEM

The information system discussed in this section has taken another pseudonym for non-identification purposes. The name POSEIDON seeks to reflect a sea of troubles with the implementation of this particular information system. This does not mean that the implementation of the system has resulted in a failure; quite the contrary. The POSEIDON system is fully operational up to the time of editing this book in January 2010, and it is one of the most important information systems of the bank to date. But as is the case with many information systems, the resulting system has little to do with what was originally intended. This does appear to be a general property of information systems: 'A system is what a system becomes; and not what it was intended to be' (Angell and Smithson, 1991). The implications for both the money laundering analysis team and AML within the bank will become evident later in this section.

The POSEIDON system was an in-house development effort, but based on another technological platform that was bought off-the-shelf from a software company. As discussed with several interviewees, the purpose behind the implementation of the POSEIDON system was to link together disparate information systems within the bank and to create a system whereby all account information would be held. Perhaps more importantly, a system where each customer would be identified with a unique identification number, namely the POSEIDON ID.

After the system's implementation, POSEIDON became a crucial information system within the bank and is currently part of the online system that bank tellers use to carry out day-to-day transactions. The simplest case where the system is used is when a customer goes to the branch to open an account. Staff would then access the system and assign the customer with a unique identification number. The system has various features that show the overall position of the customer, such as account information, deposits, withdrawals and so on. It also allows the extraction of account statistics for individual customers, and for groups of customers.

Tracing back the problems that emerged with the adoption of POSEIDON, it became evident that as the prior information systems of the bank were gradually developed, implemented and deployed, they had become an integral part of a highly complex infrastructure. In this

evolution, one immediate consequence that stemmed from the creation of highly complicated informational infrastructures was the difficulty in maintaining consistency in the database format. With the constant advances in computing, programming languages were bound to evolve (and are of course still evolving). The different information systems were far from uniform. New technologies were constantly being developed, and as new business and compliance needs were constantly emerging, variety in computer systems became unavoidable. Written in different computer languages and database structures like COBOL, PL1, DB2, and so on, these problems became ever greater when the bank decided to implement POSEIDON, yet another system where basic account information would be stored. POSEIDON became an agglomeration of data from various sources. In other words, this system was greatly affected by the variety of different databases already existing prior to its own implementation. One such database that was used to feed POSEIDON with customer information came from the bank's spin-off company that issued debit and credit cards. There were many other databases, each set up for their own, and disparate reasons. As a staff member from the Department of Organization and Management of Information Systems commented:

> That was exactly the problem. The initial process of feeding the POSEIDON system with customer information was problematic because it was contingent upon many different databases and databases themselves degrade. No database was complete in itself. The POSEIDON system inherited in this way many problems which have not so far been solved. It looks like the problems are never going to go away because the processes of rectifying them take a considerable amount of time and meanwhile new needs are being developed.

Apart from the problems that emerged after the implementation phase of the POSEIDON system, there are various other factors that influenced the system's integrity and purpose. Some accounts, which were quite old in terms of the time of opening of the account, were not part of the POSEIDON system at all. They had to be entered manually. Furthermore, the operating procedure that clearly stated that every customer should have a unique POSEIDON ID was constantly violated by staff members who would just not bother looking into the system for already existing customers. This meant that customers who went into a branch with the purpose of opening an account, but who had already opened other accounts with the bank, would simply be given an additional unique POSEIDON identification number. Instead, what the branch staff member should have done was to unite all the accounts of the customer under a single ID number in the system. Whilst interviewing personnel from the MLAT, I was even told of customers with ten POSEIDON identification numbers. One staff member

from the compliance group of the bank mentioned that she had five 'unique' POSEIDON IDs herself. On top of these issues that rendered the system's basic functionality heavily problematic, apart from basic account information that was compulsory, staff members in the branches of the bank would not enter all the customer information. Fields of information would be missing or would be entered incorrectly. Postcodes, addresses, occupations, and many other details were compromised. A multi-threaded matrix of complexity was suddenly realized, and clearly, something had to be done about these problems.

Shortly after the bank had recognized the problems with POSEIDON, a decision was made by senior management to make consistent attempts at rectifying them and to pass this particular task to the branches themselves. The Automated Centre for Transaction Recording would then query its own databases[1] and produce lists with people that had multiple accounts with the bank and consequently several different POSEIDON unique identification numbers. These printed lists would subsequently be sent to the branches, and they would have to double check the identification documents from the customers and unite the different accounts under a single POSEIDON ID. The instructions that were given to staff members would also include collecting the required information missing from the POSEIDON system. This additional information (for example postcode, occupation) was needed so that the database was as complete as possible, with the ultimate purpose of creating a single POSEIDON ID in those cases where multiple accounts existed.

According to estimates given to the author by the Department of Organization and Management of Information Systems of the bank, there are two issues worth mentioning that concern the process of rectifying the problems in POSEIDON. Five years after its implementation, it was estimated that only 40 per cent of all the accounts of Drosia bank have been added to the POSEIDON database. Out of those, and after several years of trying to rectify the problems, only half of the customers originally given multiple ID numbers had been given a unique POSEIDON ID. That number was considerably lower 4–5 years ago when a mere 15–20 per cent of the customer base had a unique identification number.

The implications for the money laundering analysis team are clear. Considering that POSEIDON is the only online system to which the MLAT has access, its use heavily affects AML work. It is perhaps worth noting here that use of the POSEIDON system is structured in a particular manner in order to allow access for security purposes, since it constitutes a key operational transacting platform for the bank. POSEIDON was designed to be used only by tellers and chief tellers, and so in order to allow the MLAT team access to all of the core information modules, they

were given permission to carry out transactions as if they were tellers/chief-tellers. This of course exposed a slight security risk had the staff of MLAT been prone to insider-fraud, but this occurrence has yet to happen. Supervision of MLAT work is very carefully managed when overseeing the entire investigative progress and when access to this system is required.

In any event, the identities of those under investigation by the MLAT are cross-checked against POSEIDON. Establishing the identity of a person under investigation becomes time consuming when there are multiple ID numbers. Basic information concerning their account balance can also be retrieved. But as POSEIDON is incomplete, further problems become unavoidable. For example, if the same person has five different accounts within the bank, and five different ID numbers within POSEIDON, every single one would have to be checked, making the process of getting an overview of the person's financial position more complex and time-consuming.

Awareness of the level of incompleteness of POSEIDON creates an additional problem when undertaking such important investigations. The team has to be certain that data is accurate and hence has to resort to contacting all the branch-network of the bank through the Fast Transmission of Electronic Messages system as a complementary step of verifying customers' identities and their accounts. The communication throughout the entire branch-network in such a way entails a series of risks. For example, maintaining confidentiality becomes more difficult with such decentralization,[2] particularly in high-profile cases that have received considerable publicity. Even though such confidentiality breaches have been very rare, they have indeed occurred.

These multiple difficulties collapse into one fundamental problem: The MLAT cannot be certain whether a person under investigation has an account with the bank by making use of POSEIDON as it is incomplete (obviously, this case is applicable only when the FIU requests information from all financial institutions for particular persons). As the manager of the MLAT team commented: 'our investigations are based on information that is far from being adequate and complete. This makes the investigative part of the work hard and in various occasions a very time-consuming process, something that is critical in cases where money laundering has potentially taken place.'

It is evident from the aforementioned comments and analysis that there are various factors that influence anti-money laundering investigations internally within the bank. Some of these problems are considerably influenced and exacerbated by the use of various information systems within the bank. These systems range from systems designed for specific tasks relating to AML (like the Case Management System) to

information systems that have a different purpose and functionality (such as POSEIDON), but which are still utilized for and are crucial to money laundering investigations.

The idea that it is only automated profiling software that is affecting AML work is quite evidently false. Automated profiling software that functions by running supposedly sophisticated algorithms that spot suspicious transactions is but one example of an information system. There are however a number of different IS-related influences that affect the result of AML-work within a financial institution. These influences come to affect the traditional organizational structures of AML-work and, to a large degree, the output of AML-investigations.

THE EXTENT AND FORM OF ASYMMETRY IN STRs

The finding described in this section regarding the asymmetry of STRs could be considered as not only one of the most critical pertaining to the systemic effects of the suspicious transaction reporting system, but also a very important one in terms of both the processes underpinning the reporting mechanisms and the manner in which they are influenced and managed. There are also considerable implications for anti-money laundering in general that will be discussed in the following chapter regarding the lack of homogeneity in reporting STRs. An attempt is made here to examine the matter analytically. Stakeholders from financial institutions are encouraged to reflect upon this type of analysis presented here as it can be rather easily applied for the identification of the asymmetry being exposed.

At this stage, and before proceeding with an examination of the distribution of the suspicious transaction reporting system, it would be useful to remind the reader of something that was discussed at the beginning of this chapter, and in particular, the observation that the number of suspicious transaction reports received by the MLAT has increased considerably over the past decade. What does not however become obvious, from any observation that has its source in aggregated statistical data, is whether – and to what extent – the entire network of branches of the bank contributes in a similar and homogenous manner to the volume of the suspicious transaction reports sent to the MLAT.

In the first place, the answer would appear to be in the negative. One could rightly expect that some form of asymmetry would be prevalent in the distribution of the suspicious transaction reports. The impossibility of a total homogeneity in the distribution of STRs is after all swiftly inferred once one considers the variety of factors (for example geographical

distribution) that come into play. But if one moves past that stage to ponder the question of what is exactly the form that such an asymmetry could take then it becomes obvious that additional empirical data are required in pursuing the answer to this question. Furthermore, the underlying reasons that gave rise to such an asymmetric character, as well as the implications for the asymmetry, become of immediate concern as issues of further research interest.

Once again, this sort of information was made available by the MLAT. Retrieving aggregated data required the help of CMS at an individual branch level, although without any statistics (or visualisation for that matter) as the software was not equipped with that functionality. When data at branch-level were manually retrieved with the help of the CMS and aggregated statistically, the problem of visualization had to be solved due to the high volume of both transactions and branches. This was achieved by using a data-mining platform with which the following results were produced. The entire process lasted for about 2–3 months.

Figure 4.3 depicts the distribution of the number of suspicious transaction reports in respect of the branch network. First of all, the actual labels from the x-axis have been removed for confidentiality reasons. The graph displayed here is only a sample, and does not include all the branches of the bank, however, the sample provided here is characteristic of the broader picture observed for the entire network of the bank. Groupings in the x-axis indicate branches of the same geographical region, while every single dot in the diagram represents an individual branch. The higher the dot is placed along the y-direction, the more suspicious transaction reports have been reported from that particular branch to the money laundering analysis team of the bank.

From the distribution of individual branches along the y-axis, it is evident that the vast majority of branches within the network of the bank are almost inactive insofar as reporting suspicious transactions; that is, the vast majority of the branches send extremely few suspicious transaction reports in contrast to only a handful of branches that produce the bulk of STRs. The reader is reminded once again that although only a sample, the above graph remains representative of this asymmetry throughout the entire branch-network of the bank. The form of the asymmetry and lack of homogeneity in reporting can now be better articulated. It becomes evident that when one examines this submission of STRs throughout the bank-network, then the degree of asymmetry that branches exhibit in the reporting of STRs requires further pondering and investigation.

When the above finding was discussed with both the manager and the assistant manager of the MLAT, as well as personnel within the MLAT, it became evident that all were of course aware that some asymmetry like

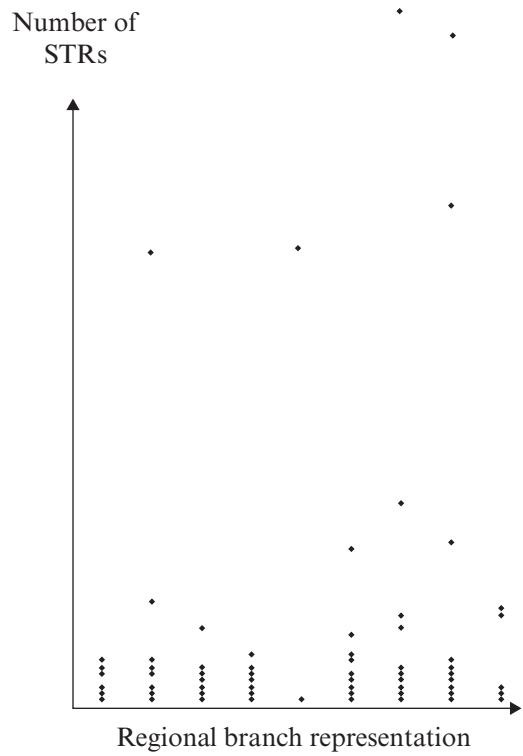

Figure 4.3 STR-submission asymmetry in the branch network

this would exist; they said that some branches are more active in sending suspicious transaction reports than others. But as this was the first time that this data – in this form – had become available and that the problem was exposed throughout the entire-branch network of the bank at such a scope, no initial satisfactory explanation could be provided as to why such a large number of branches were inactive in reporting. This led to a subsequent investigation by the author, for which additional data-mining of the extracted dataset was carried out in order to determine the percentages of the distributions for which STRs have been sent from individual branches.

The purpose of this additional examination was threefold (even though the following elements are interrelated): a) to identify the percentage of the branches that have sent no suspicious transaction reports whatsoever, b) to identify the percentage of the branches that have sent very few STRs, c) to identify the pattern of distribution that stretches from those groupings

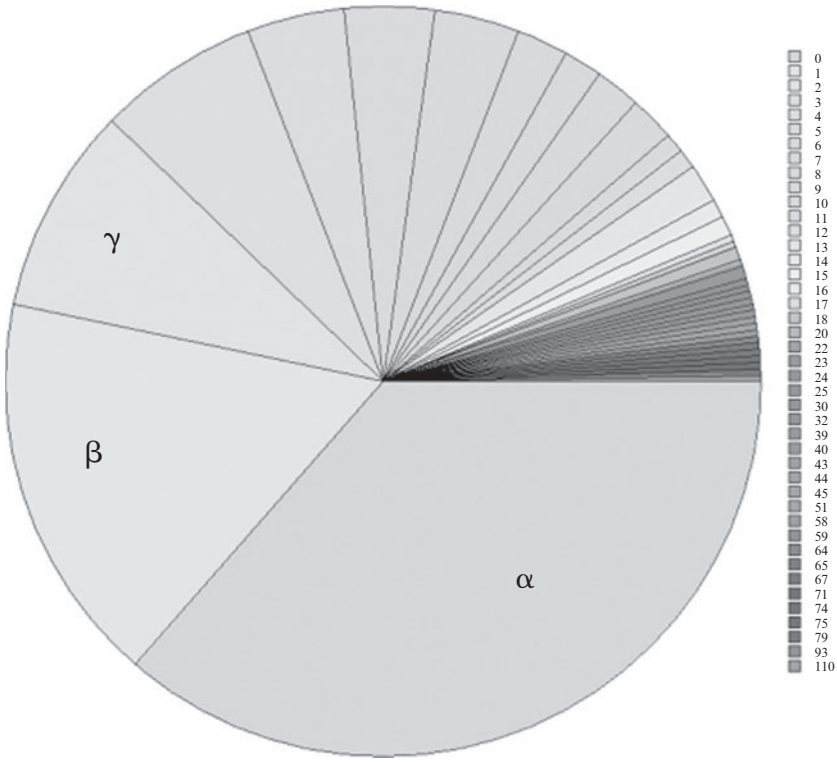

Figure 4.4 Asymmetric distribution of STRs in aggregated categories

of branches that have sent very few suspicious transaction reports to those that have sent the bulk of the STRs.

Once again, the same data-mining platform was used for the categorization of branches with the same number of suspicious transaction reports; this produced the graph shown in Figure 4.4.

It has to be made clear that the actual numbers of how many branches are in each category are not made available for anonymization purposes, but the percentages are clear and hopefully of striking importance! The categories on the right part of the graph are the number of STRs that correspond to the different shading of the graph (starting with the shade that corresponds to the **α** category and moving on clockwise to **β**, **γ**, and so on). Categories match the distribution pattern clockwise with the first category indicating that the largest percentage grouping are the branches that have never filed an STR with the MLAT, the 0 (zero) STRs category.

Similarly, as indicated from the pie chart, we can see that more than 50

per cent of the branches have either zero or one STR throughout the whole history of AML in the bank. We can then make the following observation: As the number of suspicious transaction reports increases, the distribution becomes denser. At the far end of the distribution (clockwise) we have branches that have submitted a large amount of STRs. This implies that the vast majority of STRs comes from less than 8 per cent of the entire population of the branch-network!

Several interviewees have given different but complementary explanations as to why this form, type, and extent of asymmetry can be observed. Their interpretations are of considerable interest. As one of my interviewees from the MLAT commented:

> Those branches that are over-reporting are simply those branches that are sticking to the letter of the bank's policy, which has of course been formulated in accordance to the guidance from the central bank. These branches are therefore typically clear with their obligations and simply operate very formally. It is the other number of branches that haven't reported anything that should concern us. Those branches that have been quite moderate in reporting also put some judgment in before sending an STR.

For this issue, the MLRO commented:

> Let us not forget that training (which proceeds gradually) is an important issue here and some sort of asymmetry was expected. But obviously, this is too much. What I expect in the future is that more of the branches that have been somewhat inactive will send more and more suspicious transaction reports. Clearly, there needs to be considerable thought on how such an increase will be handled, for which additional resources will be required (resources that we have already asked for). The impact that technology will have is also something that we have to consider. Imagine what would happen now if we gave to some of these people in the branches that are over-reporting the possibility to report to us the suspicious transactions electronically. We wouldn't be able to cope because of the massive volume of STRs and the backlog would be tremendous. Reporting is going to skyrocket and the employees are going to take few chances.

A testament to such problems and an additional fact to be considered is the effectiveness of those branches that were over-reporting. Following the reflections and comments for the form of asymmetry in reporting STRs, a sample was chosen in order to examine the percentage of unsuccessful reports (those that, after careful manual examination by the MLAT, were deemed to be unworthy of further escalation and reporting to the FIU). As the software used within the bank (the Case Management System) did not allow for the extraction of such statistics at a branch level, manual examination of each individual branch would have had to be undertaken in order to produce statistics representative across the entire branch-network

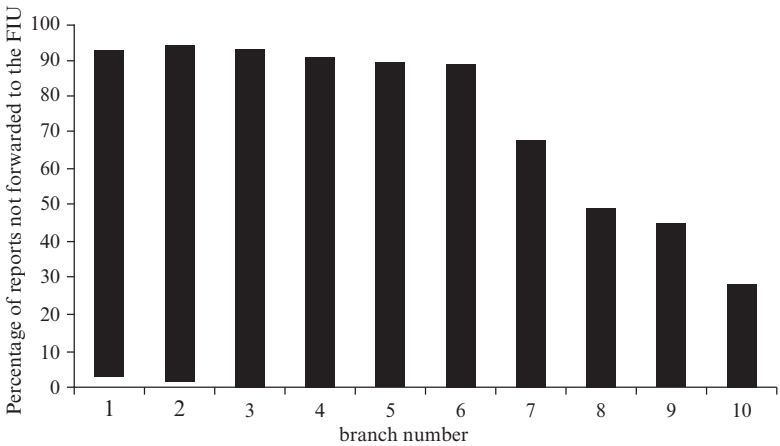

Figure 4.5 Top 10 most active branches in reporting and percentages of unsuccessful reports

of the bank. As this would be a cumbersome process, a small sample was selected of the ten most active branches in reporting STRs in order to examine further the percentage of those reports that were deemed to be unsuccessful and were subsequently archived in the CMS without further escalation or reporting to the FIU. The top-ten most active branches in STR-reporting are displayed in Figure 4.5.

From Figure 4.5 we can observe that amongst the top ten branches in reporting activity, the first six have a considerably high percentage of unsuccessful reports of around 90 per cent. This means that only one in ten reports is considered to be suspicious enough to be sent to the Financial Intelligence Unit after careful manual analysis from the MLAT and the MLRO's final decision.

A considerable implication that is of qualitative nature and cannot be easily quantified becomes the impact of such dynamics of STRs to the MLAT that is responsible for their analysis. For example, how is the MLAT influenced by receiving a report from a branch that has a 90 per cent failure rate in reporting? Could the risk-based approach be extended to include this type of granularity, where individual branches would be scored on success rates of STR submissions? Are there any circumstances under which reports from such branches become prejudiced following a series of unsuccessful reports? Regardless of the answer to such questions and the qualitative subtleties or personal judgments that could be involved, it quickly becomes evident that a risk-element is prevalent here. Therefore intelligence gathering that points towards effectiveness in reporting STRs

from individual branches could be further used for consideration and integration with a risk-based approach in reporting, something that could become very useful in light of the projected increase in suspicious transaction reports. Other branches, however, appear to be far more effective in their reporting (even though the number of STRs that these branches send to the MLAT is a little lower compared to those exhibiting a higher rate of unsuccessful reports).

Interesting as this observation may be, the study of identifying at branch-level what those elements might be (whether those are working processes, training methods, staff demographics, statistics, or anything else) that are strongly related with a branch's relative success or failure in providing useful STRs to the MLAT, is a set of matters that is somewhat different in scope from the issues that this book set out to examine and one that would require considerably different methodological techniques. Indeed, this could be another research agenda in its own right.

Thus far, the internal reporting system of the bank as well as the reporting implications towards the FIU, the different ways with which investigations can be led, as well as clear implications of information systems within AML have been examined in some detail. Two such examples came from the Case Management System of the bank where investigations for AML are logged, as well as the POSEIDON system that is used throughout the bank for uniquely identifying customers. As this chapter comes to an end, it will proceed with a more forward-looking topic (as far as Drosia bank is concerned) that is related to new automated solutions for anti-money laundering, the implications that these exhibit, and the influence that they have.

THE CHIMERA SYSTEM: A NEW AUTOMATED SOLUTION FOR AML

First of all it has to be made clear that in the particular financial institution being investigated and the national context under which it operates, no initiative was taken from the central bank to urge the financial institutions towards implementing and adopting profiling or other AML-related technologies. Every single financial institution acted on its own initiative, and therefore some variety can be observed in the banking sector. Some financial institutions have already bought automated solutions while others have built their own software for monitoring suspicious transactions.

Drosia bank has had (as already discussed) a series of information systems, but never a centralized and bespoke system targeting the automated identification of suspicious transactions for money laundering. Even though the focus of this book lies broadly in the technological

structures that can affect AML, and not explicitly in profiling, data-mining or other risk-oriented software for AML, it is important to describe the story behind the CHIMERA system, one of the latest systems to be implemented in the bank.

As profiling technologies for AML were becoming fashionable around the world, and the software houses providing them truly successful in gaining disproportionate financial gains to their efforts, Drosia bank and many other banks at the time, started looking for automated and profiling solutions for AML. These solutions would typically claim to act in an 'intelligent' manner, thus capturing the 'behaviour' of money launderers, and through a series of techniques that could go under the most mystical of names to the uninitiated (neural networks, artificial intelligence and so on), software claimed considerable success in targeting money laundering, a success-bubble that soon burst (Demetis and Angell, 2006).

Still, the decision to look into buying a software package was taken at the bank as some ongoing problems regarding the monitoring of STRs had to be addressed. Internet banking for example was not monitored for money laundering at all; nor was it scrutinized in any way unless particular cases were brought to surface from other routes such as an STR from one of the branches of the bank and then specific searches would be carried out to observe the pattern of transacting from online banking. It was similar for ATM transactions. Discussions commenced in the year 2000, and continued up to the year 2004. During this period, and following this initial line of interest into the purchase of a software package, the Managing Information Systems Department of the bank took the initiative of requesting representatives from various companies that supplied software of that type to present some of the inner-workings of the software and the underlying functionality. Major companies that presented their AML solutions to the bank included (without this list being exhaustive): Norkom, Unisys, Hughes Financial Analysis, Thompson Financial Services, SearchSpace, IDL, NetEconomy and Mantas.

When asked to comment on the functionality of AML software that was presented to Drosia bank, the Deputy Director of the MIS department of the bank commented the following:

> The vast majority of AML software that were presented to us were overly complicated and either did a series of things that we would never ever need, or were incapable of being customised to the extent that we would want them to be, something that will prove crucial in the decision to buy one. To give you an example of what I mean by overly complicated we don't need to go far as this is a phenomenon I have observed in software packages throughout the last years. If you take Microsoft Word as an example, it quickly becomes evident that justification of different versions, updates, and so on that would justify the cost (or

> the increase in cost of the package), have overloaded the software with a series of things that nobody hardly ever uses. There are more than 200 features and options in Word. How many do you actually use? How many does anyone actually use? Well, the way I see it is this: AML-software are the same. Too much functionality, but no actual difference in its efficiency.

Interestingly enough, according to my interviewee from the MIS Department of Drosia bank, while the negotiations were taking place regarding the various technological platforms that could be purchased, an analyst from a company that was presenting their AML software platform was attributed with the following quote: 'We know that the problem is very difficult and we must admit that no profiling technology actually works. Ours is relatively cheaper and you need it for demonstrating compliance. That's all!'

That analyst was spot on. Technology as a means of demonstrating compliance and willingness to deal with AML seriously has nothing to do with the actual functionality of technology itself. When the process of consulting with software companies regarding AML solutions was completed, the decision was eventually made by the management not to buy one, and a firm choice and commitment was made that opted for the development of an in-house component that would be part of the POSEIDON information system; one that would be most closely and explicitly related with money laundering prevention and investigation. This turned out to be a system that will hereinafter go by the name CHIMERA, whose scope will be examined here. In several interviews in the MIS department of the bank, the decision not to buy an off-the-shelf software platform for AML was discussed. Several reasons were identified:

1. A major problem was the poor interoperability of the software package with the already existing infrastructure of information systems that operated in the bank. The complexity of the endeavour would be overwhelming as more than 50 subsystems operated and the solution (of achieving interoperation and hence increased interoperability) would have to be achieved through a series of middleware, thus introducing even more complexity and in various cases reducing the functionality of the software package provided.
2. It was believed that many more problems would emerge if the software was bought off-the-shelf. On the contrary, it was viewed that in-house development is much better, particularly when one sees beyond the software packages that were presented, and comes to the realization that there is an underlying core functionality that is truly very basic (and that the bank would not really need any more than that for compliance purposes).

3. Beyond the integration and interoperability of the software, an additional problem was the administration of the system, and the profiling rules that would be used for monitoring money laundering. There was considerable ambiguity over whether the software companies had actually delved deeply enough into the issues of ML-modelling, or if the construction of their profiling solutions was a simple automated transfer of a huge number of typologies.
4. A further issue that contributed towards the decision of not buying a software platform was that on a large number of occasions, more centralisation at the level of both STRs and transactions would adversely affect the MLAT. This would considerably change the KYC balance of the internal STR-regime of the financial institution, and hence it was viewed that the MLAT should not carry this burden. This was of course a matter of emphasis, and it is worth noting that different financial institutions have different perspectives on this issue. For Drosia bank, the locality of branch-level knowledge was more important for scrutinizing suspicious customers than a centralised software platform. It was viewed that the KYC responsibility lay mainly within individual branches.
5. Finally, an important reason to decide against an off-the-shelf solution was the cost. It was simply much cheaper to do it in-house.

Despite all these objections to the purchasing of off-the-shelf software, the bank went ahead and bought one profiling solution in the year 2007 (more on that later). Meanwhile, the in-house development of the CHIMERA system came to fruition and the system became operational in 2005. The specifications of that software were discussed with a series of interviewees, both from the MLAT and the MIS Department of the bank. An attempt is made here to consolidate the results of these interviews in order to discuss some aspects of the software-functionality and its consequences:

1. The core function of CHIMERA (initially at least) was to provide a platform that would connect to all online systems of the bank, but mainly POSEIDON. CHIMERA is essentially a database of suspicious names of individuals and companies that are consolidated and interrogated from other systems in the bank. So far, three lists are used to feed information into CHIMERA; the internal-updates of these lists customized for the bank can only be updated by the money laundering analysis team. These three lists currently are: the CFSP list from the European Union, the OFAC list from the United States, and a complementary list from the central bank that basically forwards

FATF requirements and countries that are sanctioned in the NCCT list.

2. The CHIMERA system is not directly associated with profiling for money laundering, and there are no immediate plans to attempt behavioural profiling within CHIMERA, other than to check for smurfing, which is done centrally once per week, but which is not within the function of the system itself. At a second phase of implementation, the CHIMERA system will provide for the monitoring of suspicious transactions, including identifying the thresholds at which transactions should be screened more carefully. However, this is likely to be delayed in its implementation because of the potential consequences a considerable increase in the number of STRs might induce. Profiling attempts, when they materialize, should be within the scope of the money laundering analysis team where there is considerable intelligence about suspicious cases, namely those cases recorded on the Case Management System.
3. Part of the functionality of CHIMERA is essentially to interlink with POSEIDON. Transactions that are being performed by tellers are automatically screened for suspicious persons against the CHIMERA system. If the customer is found in one of the suspicious lists then the transaction is automatically blocked and a chief-teller/manager has to be informed, who then takes responsibility for further informing the MLAT of the incident.
4. It is useful to note that one of the problems discussed was that the tellers always find the filing of a suspicious transaction report to be a cumbersome process, one that takes a considerable amount of time. This was discussed in relation to the possibility for the electronic submission of STRs via the CHIMERA system. Even though the MIS department of the bank was in favour of integrating a module for the electronic submission of STRs by tellers, the MLAT and the compliance department of the bank were against this option, as it was (and still is) believed that it would considerably undermine the KYC process, which is considered to be paramount. Despite this however, the option of electronic reporting was built into the CHIMERA system for potential future implementation, but this would also require the development and implementation (along with training and use) of electronic signatures for employees, something that has not been provided thus far.

Following the design and implementation of CHIMERA, a few problems started to surface that are worth discussing in brief. Some of them were systemically emergent, and others were due to organizational

problems and lack of sufficient coordination. Despite the fact that the initial feed into the CHIMERA system was done automatically from the CFSP and other lists, and that the format in which the lists were available was the highly-interoperable Extensible Markup Language (XML), no provision whatsoever was made for updating the list in an automatic fashion from the MIS department of the bank. It was believed that the initial feed of data would be a cumbersome process, and that consequently slight modifications would be required. This meant that the whole task of updating the CHIMERA system would have to be undertaken manually, and so the task was passed on to the MLAT.

Following an interview with a manager in the MLAT it became evident that the original estimation that updates to the CHIMERA system would be minimal, even though done manually, was an underestimate, to say the least. 'Suspicious' lists can always expand rapidly in the case of scandals. Belarus[3] was a classic example where corruption led to a series of sanctions and the inclusion of a wide number of individuals in the blacklists. Inclusion of these lists in the bank's systems required manual input of the names and details of all those involved; this became a cumbersome process that took considerable time away from some critical working tasks and investigations. Furthermore, shortly after the CHIMERA implementation, it was realized that the Case Management System (CMS) where STRs from the branch network are recorded, also required the input of suspicious names from the widely available lists. Difficulties in the way the CMS functions, and failure to address the issue of the interoperation between CHIMERA and the CMS, meant that manual input from lists of suspicious persons and organizations became unavoidable, and the process of manually inputting was further duplicated in order to update both the CMS and CHIMERA.

This lack of interoperation between the CMS and CHIMERA exposes further the lost opportunity of gathering intelligence on ML behaviour. The fact that the CMS contained details of all cases that have been investigated for money laundering from the very beginning of operations of the MLAT and the computerization of their work, meant that there was a wealth of information that could have been exploited for intelligence purposes within the financial institution itself. Since the CHIMERA system was essentially a way to manage a particularly structured risk (with this risk being a scenario in which customers in any suspicious lists would attempt to transact with the bank), similar risk-management paths could have been drawn alternatively with the help of the CMS and/or with an interoperation between the CMS and CHIMERA. In negotiations between the MLAT and the MIS Department of the bank, this option was never requested and an opportunity was missed for the integration and use of intelligence between the two systems (old and new).

It was not only the CMS that was affected by the introduction of CHIMERA; the underlying functionality of CHIMERA interfered with the functionality of the Fast Transmission of Electronic Messages (FTEM) system. The reason is rather simple; instead of sending messages that included suspicious names to all branches in the bank through the FTEM system, those names were simply loaded into CHIMERA. In case tellers attempted to carry out any transactions in which any of those names were involved, the transactions would be stopped by CHIMERA, the teller would be prompted to call for chief teller/manager's assistance, and the latter would notify the MLAT for further advice. Despite the obvious overlap between the two systems, following a series of interviews post-CHIMERA implementation, it was clear that both systems were operating simultaneously and independently, and that CHIMERA had done little to replace the FTEM. The overlap however was striking, and the MLAT decided to examine whether the scale of usage of the FTEM in handling suspicious lists could be minimized. Going through the CHIMERA manual, and discussing this issue with a staff member from the MLAT, the reason that the overlap was hard to resolve became clear: the CHIMERA implementation that affected the online transactions of Drosia bank was restricted to a series of transactions (transaction codes to be more specific, where for instance the act of depositing money into an ATM machine may constitute one single transaction code) that did not encompass the totality of the transaction codes within the bank. Coupled with the incompleteness of POSEIDON, with which CHIMERA was linked, a complex network of system interdependencies emerged in the handling of suspicious lists. It is worth noting that whereas there is only a handful of transaction codes that are checked online and real-time against the transactions that tellers attempt to carry out, the remainder of the transaction codes that are not linked to POSEIDON are checked against CHIMERA once a week for all the clientele of the bank and for all transaction codes. In the event someone has not been spotted via other means, batch processing will uncover it, even if somewhat later; this is of no consequence since there is no requirement whatsoever that imposes a time frame for the reporting of suspicious transactions.

But even within individual transaction codes that were linked with CHIMERA, further unexpected problems emerged. The capacity to send Society for Worldwide Interbank Financial Telecommunication (SWIFT) messages is such an example. Due to a particular structuring of the SWIFT messaging service, input must be constructed in Latin characters in individual lines that are checked one by one against CHIMERA. If the recipient is 'Demetis International Industrial Company' and due to the length of characters in the recipient name the last word (Company) is moved to a next line of the SWIFT message then that is individually checked by CHIMERA against

all suspicious entries that contain the word 'Company' within any of the lists – and clearly these are a substantial number (as many as are companies). All generate an alert! When this problem was realized, an exclusion of keywords from CHIMERA was deemed to be the optimal solution for resolving a large number of alerts in the online transacting system of the bank, otherwise tellers would have to face an increasing number of alerts that did not correspond to any suspicion. A draft list of keywords to be excluded was put together. This list included words like: import, export, company, industry, bank, trading, insurance and tours. Eventually, the MLAT was told that the exclusion of keywords did not stand possible. To this date, whenever a SWIFT message is sent and this problem emerges (if it happens and one of the popular words make it on a separate line), an alert is generated and the teller has to take action to bypass the problem. The supervisor in the branch is then called in to confirm that this is not suspicious and the transaction can go through.

An additional problem that was realized in CHIMERA, insofar as it was interlinked with POSEIDON, was the matching of suspicious persons provided in the CFSP, OFAC lists that are delivered in Latin-based characters, and with those kept within the POSEIDON system in the characters of the national language used in the country. For example, if an institution operates in Poland, and since accounts and database structures would be in Polish, there ought to be a conversion to the national language character-set. The same for Finland, Spain, France, Russia, Greece, and so on. As the author's nationality is Greek, an example will be provided in the Greek-language-set and the author's last name will be used as an example to highlight the problem that was faced. An automatic routine was employed to convert the names from the Latin-characters of the OFAC list to the characters within POSEIDON. Let us suppose that this example were to take place in a Greek financial institution. A sample of letter-to-letter correspondence is provided below:

A → A
B → B
C → K
D → Δ

It was soon realized however that such an automatic conversion came with several problems. In a standard check for OSAMA BIN LADEN by using only the keyword LADEN in the system, if one were to type the LADEN in – say Greek characters – then no alert was raised whatsoever in any of the transacting codes! It was immediately obvious that something had gone wrong in the conversion of the name, something lost in the translation, and that had Osama bin Laden transacted with the financial

institution by electronic means (clearly a hypothetical scenario), the transaction would have gone unnoticed. Looking at the conversion list it became clear that in the particular scenario, the 'D' letter in the 'LADEN' would require two letters so that the pronunciation can equate to the English equivalent and that these two letters would be 'NT' if we stick to our Greek example. Phonetically then, 'D' in English that is equivalent with 'NT' in Greek would require the conversion D→ NT. The exact same problem on a different character-set was quickly rectified for CHIMERA in this case and the conversion was re-run.

As with any automation (the example in this chapter in the initial feed of information into the POSEIDON system is typical), problems may percolate within the system that can only become obvious after the event. Let us suppose that the author's name was in one of the suspicious lists, and an MLAT-member was looking for it in the CHIMERA system. Following the automation rule for LADEN then the author's last name 'DEMETIS' would have been 'ΝΤΕΜΕΤΙΣ' by following the automated conversion. The real spelling of the author's name in Greek however is 'ΔΕΜΕΤΗΣ'. Here we observe the following: D can be either Δ *or* NT.

In such a scenario therefore, differentiation between the two requires an extra proxy that can be connected to the conversion of the name, another difference in itself. Nationality for example could be such an extra proxy for determining the difference of the difference, but it quickly becomes obvious that within any proxy there are other differences that would require other proxies in themselves. The problem of identity and establishing one's identity is never as straightforward as some view it to be, and it is definitely not something to be seen as a unitary package. Identity is a set of attributes that we use to refer to someone and therefore it depends upon the choice of attributes and the variation these exhibit. Particularly within the scope of language, and the multilingual needs that have been posed by globalisation at an alarming pace, interesting research is currently addressing this problem area.[4]

The problem, trivial as it may initially appear, becomes considerably more complicated by the vastness of data structures where trillions of records are stored, and require automation in their handling. No database is perfect and error-free, and as has already been mentioned, precisely because of the underlying complexity, databases in themselves degrade. New needs are developed that require a change in the structures, while the new needs require integration and interconnection with previous structures that are, in themselves, incomplete.

It then becomes obvious that interconnections and the interdependencies between any two systems that need to be connected pose both structured problems that must be studied thoroughly by analysts and resolved where

possible, and also unstructured problems that emerge from the interaction between the systems and cannot be attributed to either system; the very act of interaction comes with complications that become far more important for the systems themselves and those that depend on their functionality.

THE ELECTRONIC UPDATES SYSTEM

As this chapter gradually comes to an end, right before some broader comments about the bank are presented and before we move on to the discussion, it is useful to note that a very important aspect in AML concerns the manner in which employees of the financial institution receive information and updates. Such updates involve changes in internal guidelines, policies of the bank and other AML-related news.

A system that is used by employees to receive new information items is the Electronic Updates System (EUS). All employees have access to the EUS through the bank's intranet. Next to each individual information item there is a box that the employee must tick to indicate that he or she has been informed of the specific information item: and the process is repeated ad nauseam.

Most of the remarks made by interviewees regarding the EUS pointed to the fact that it is very difficult to carry out a timely distribution of critical new information items or guidelines to the bank tellers, even when EUS is utilized. Tellers have an extremely limited amount of time at their disposal whilst working at the bank, and it has been observed that it is commonplace for employees (and in particular bank tellers) to acknowledge that they have read the relevant guidelines by ticking the boxes related to each guidelines, whereas in reality they had no time to be informed about anything at all. This becomes a considerable problem in day-to-day operations that remain one of the most vital fronts against money laundering. The EUS is meant to allow branch managers to see whether their employees have been informed about the new information items and of an analysis of who has been informed of what. However, branch managers too are confused about the functionality of this system (in conjunction with the time-restrictions that are in place) as they find it difficult to control the process and to make any sound inferences of who has been really informed of the new guidelines.

THE ZEUS PROFILING SOFTWARE

On top of the complexity generated by the interference of all these AML-related technologies, Drosia bank eventually succumbed to the pressure of

the market and made the decision to buy an off-the-shelf AML-solution even though the original decision was against that and despite an original commitment to develop and use CHIMERA. With CHIMERA already functioning, the off-the-shelf software (ZEUS) was introduced in 2008 and its introduction to the bank was accompanied with a consulting period of 1.5 months. The company that originally built the software offered the consulting services. It might be added here that the particular software platform is one of the most popular AML software 'solutions' globally. In any event, both this limited consulting period, as well as the lack of AML-expertise from the consultants of the software company were a disappointing combination for Drosia bank that dealt with another layer of complexity.

Nearly a year and a half after the introduction of the ZEUS profiling system, the totality of the parameters available in the form of raw transaction data was not implemented. While the software itself had the capacity to operate real-time in order to block suspicious transactions, it was reduced to an overnight batch-processing function. The current time lag is one week between the batch-processing of reports and the manual scrutiny for KYC purposes. The OFAC and CFSP lists of suspicious persons are not integrated within this particular software but are instead used as part of the CHIMERA system and are updated manually. The POSEIDON Information System is not integrated at all within ZEUS, and hence considerable fragmentation exists at account-level information that could be used for profiling purposes.

Hence, the AML-group of Drosia bank is currently coping with the fine-tuning of the operative functions of the profiling software problems. Ironically, the software companies that are responsible for the construction of these technology-based platforms call them software 'solutions'. But they do create a number of problems for the individuals responsible for AML-based processes.

With these introductory comments in mind, the current status of the integration of the profiling software within Drosia bank is presented here in brief:

The current daily output of suspicious transactions from the ZEUS automated system is running steady at 2000 STRs per day! This is undoubtedly a staggering amount of STRs that need to be manipulated intraday. Of course, the profiling software generates many more STRs but these remain hidden since the graphical-user interface of the software only allows for the first two thousand reports to be shown/manipulated. In contradistinction to this enormous volume of STR-production by the software, the capacity for manual scrutiny of the reports by ML-analysts is limited to about 100 STRs per day. These 100 STRs are selected out of

the 2000 daily output on the basis of a risk-score produced by the ZEUS software; the risk-profile that the software uses is based on a combination of assigning particular types of risk on the basis of proxies like: country-based transaction, transaction categories, amount of transactions. At the moment, no customer data has been integrated and therefore no risk-based treatise can take place on the basis of the customer's personal relationship with the financial institution (for example time of association with the bank, demographic data, and so on).

With a daily output of software-generated STRs in the vicinity of 2000 STRs per day, this brings us at about 60 000 STRs per month. According to a senior staff member overseeing the ML-analysis team, the real suspicious cases are about 10 cases per month (with actually one really interesting case over the past year and a half). Overall, the True Positive Rate (TPR) for the ZEUS AML software is around 0.017 per cent. Disappointing? Yes. But not really unique; most financial institutions start off with true positive rates of this sort and after years of experience and fine-tuning of the software, they manage to reach a state of equilibrium where the output of software-generated STRs is not totally useless to the ML-analysts who scrutinize the reports manually; in other words, they reach an average of around 4–5 per cent in the TPR. Not that it makes a big difference anyway since that too is extremely limited. It implies a huge waste in human resources: the ML-analysts in particular that go through hundreds of STRs in order to determine only very few that could be suspicious. Despite all these problems, the technological instrumentalism underpinning these processes has hardly diminished. The belief that there is a technological solution to the problem is enough to bypass the pragmatic side-effects of technological implementations across a wide number of stakeholders.

BROADER COMMENTS

Despite considerable delays in the improvement of the overall AML system, it becomes obvious that Drosia bank has established considerable working processes around anti-money laundering, and the interests of the bank often surpass mere compliance purposes. Genuine interest is shown in improving working life around AML, improving efficiency and effectiveness, and further targeting the problem domain that presents so many diverse challenges. It would be fair to say that all the interviewees of the bank saw the AML domain as a challenging problem area and the multiplicity of difficulties they are faced with as an interesting intellectual experience.

However, Drosia bank is subject to different influences, some from

within, and some from its immediate environment (FIU, central bank, and so on). Being subjected to often unrealistic demands from prosecutors or FIU (such as providing all transactions from the time of opening of the account, and irrespective of any threshold), Drosia bank unavoidably operates within a bureaucracy that is often posing considerable constraints, one that often restricts innovation because it preconditions the structure that needs to be considered before any change is done. This is something that supports the creation of an internal bureaucracy that is required to sustain the working processes.

In this regard, the information systems that have been examined here in some detail create a truly complex fabric of influences on the AML operations of the bank. As already discussed through various examples that include POSEIDON, the bank's case management system, CHIMERA and ZEUS (amongst others), the AML processes that are supported by information systems succumb to a complexity, and they influence each other in ways that are often surprising. Such processes, the information that surrounds them, and their outcomes, are never straightforward in the causal sense.

In this regard, the study of the internal suspicious transaction reporting system has been considerably revealing. The extent of its asymmetry in the branch network of the bank, the increase in the number of STRs, the respective consequences in information management, and its handling, all create a set of phenomena that characterize part of the complexity of the AML-setting for this financial institution. But the confrontation with such a complexity becomes a system in itself; it has to be reduced if it is to be communicated, and aspects of it utilized for decision-making changes within the system that employs its operations.

In the chapter that follows these aspects are brought together and the systemic complexity is eventually confronted by combining systems theory with the insights provided by the empirical findings in this present chapter. By laying down a theoretical path that confronts the way in which technology participates in the broader societal order, the links between systems theory, AML and technology are systemically expanded. These lead further to some interesting insights regarding the risk-based approach and also some hands-on applications that are presented in the final chapter.

5. Systems theory – a theory for AML

INTRODUCTION

In this chapter, the case study findings are discussed and a theoretical treatise is developed. In such a treatise, the anti-money laundering domain is portrayed as a system in the tradition of systems theory. On the basis of empirical data collected from Drosia bank, the role of technology in the AML system is also reflected upon. While this theoretical investigation attempts to establish the academic nature of AML research by moving the domain past ad hoc descriptions, one thing should be made crystal clear from the start; there are considerable implications for practice by dealing with AML in a systems theoretical fashion. This will become more evident in the following chapter where a risk-based application of systems theory for data-mining suspicious transactions is presented. An attempt is made here to synthesize the two distinct poles that have been presented thus far: the core theoretical aspects of systems theory and the more practical aspects that have been outlined for AML through the case study. Some opening remarks will hopefully be of use to the reader by providing a set of clarifications for the analysis itself.

The synthesis between AML and systems theory is carried out in two distinct phases. First, some broader comments are provided on how anti-money laundering can be viewed as a *system* through *systems theory*. This builds on previous work that attempted for a first time to merge systems theory with AML (Angell and Demetis, 2005). Second, such a description is revisited to provide a novel conceptualization of the domain by positioning AML within the systemic schema of the functional differentiation of society, and clarifying how such a differentiation constructs AML in a completely different manner. Finally, with the help of systems concepts from Chapter 3 and empirical evidence presented in Chapter 4, the role of information systems within the domain of AML is discussed. The role of technology in the construction of the suspicious transaction reporting system is analysed, the communication of suspicious transaction reports is explored, and also, a theoretical basis for the risk-based approach is developed. Even though the next chapter is entirely dedicated to the risk-based approach, some theoretical concepts outlined in this chapter will assist the reader in gaining a deeper understanding of the concept of risk.

THE SYSTEM OF AML

While the word *system* has been one of the most abused, misused and misunderstood words of the English vocabulary, there is nothing vague in the word 'system' within the context of systems theory. Even though the concept of *system* has been hijacked from its initial theoretical provinces to be used in various disciplines or in everyday life, Chapter 3 has already outlined both the foundations that give rise to the concept of the system and the interrelated theoretical concepts the existence of a system assumes (that is boundary, environment). While it is true that the definition of a system is always an observer-relative process, and that an observer may define a system differently, there is much to gain from complementary insights. Even though the unit of analysis within this book can unavoidably be associated with the single financial institution that has constituted the case study (Drosia bank), systemic considerations cannot be restricted to a unit of analysis for a series of reasons: no system exists in splendid isolation as analysed through the fundamental distinction between system/environment. Also, cause-and-effect relationships between systems and their environments are shattered by the forcefulness with which complexity replicates within systems and their respective environments.

This complexity that is exposed on the basis of the empirical findings of Chapter 4, implies that there is a considerable need to stray away from a tidy demarcation that is typically projected within the broader domain of AML. Such a tidy demarcation projects a hierarchy of AML stakeholders that function according to well-specified rules, and where problems can be overcome by specifying further rules or by introducing new legislation. Within AML, such a hierarchical modus operandi is observed in various ways. The governmental and regulatory views are typical of such a stance, whereby the broader AML system is neatly decomposed into three distinct levels, each containing a variety of organizations. These levels can be designated as follows: the local, the national, and the transnational.

Transnational organizations (UN, EU, FATF, IMF, and so on) are considered to be responsible for norm-production and believed to be constitutive of the broader AML domain itself. At the very least it needs to be recognized that they generate much of the initial momentum of acting on AML/ML, regardless of what mechanisms they use for the diffusion of such momentum and the monitoring of measures' effectiveness. Such institutions are supposed to have greater regulatory, administrative and supervisory powers than those at the national level, but such a statement could very well be viewed as a value judgment that has been institutionalized and enforced by governmental momentum. 'Greater' power in this context becomes irrelevant. Does 'greater' power imply more 'control'?

If yes, then how is that 'control' supported and exercised? Even more importantly, *to what degree do processes exist that counteract such a top-to-bottom demarcation of control*? Do they create additional difficulties for the domain of AML itself? We will see in due course how such processes come into being.

Following the transnational level, national level organizations are in this regard viewed as the next step within the three-level hierarchy of the broader AML domain. Organizations at this level have to comply with the norms that are set at an international level while they also monitor institutional stakeholders at a local level. Examples of organizations at the national level would be: Central Banks, Financial Intelligence Units, Tax Collectors, Law Enforcement Agencies and Company Registrars, while financial institutions, exchange bureaux and so on, constitute some examples of local stakeholders.

Such tidy hierarchical thinking of the broader anti-money laundering domain as shown in Figure 5.1 is clearly an oversimplification of the complexity surrounding AML. The large number of stakeholders involved creates a complex set of interactions that diverges from such a linear method of differentiating between AML-levels. This implies a shift in focus, not merely a change in terminology. By adopting the systems theoretical approach one is forced to submit the AML domain to a variety of internal and external influences that may not seemingly have a causal effect on AML. The idea therefore behind the three-level hierarchy constituted by transnational, national and local stakeholders needs to be abandoned.

Systems cannot be described by hierarchies or by linear processes of

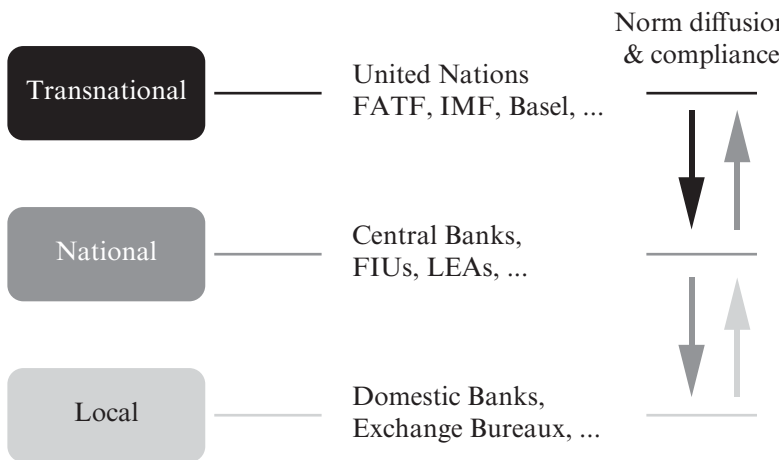

Figure 5.1 The standard model of the three-tier hierarchy

norm-diffusion. Levels become inappropriate. This means that the AML-system cannot be characterized as the totality of the local, national and transnational stakeholders. By treating the stakeholders (say a financial institution) as systems, one needs to escape the edifice that is mere compliance of well-formulated rules and move towards an examination of the underlying processes that fuel the complexity of the system itself. Systems then become *islands of reduced complexity* as analysed in Chapter 3. The reduction is necessary for observation to proceed, but that does not mean that there is a disregard for the complexity within the system. Internal processes that generate complexity out of complexity, and ultimately, risk out of risk, become the centrepiece of discussion and analysis.

Within such a systemic approach, the tidy demarcation of AML levels must collapse and give rise to a loose assembly of institutional subsystems. These are intended to combat the phenomenon of money laundering through coordinated activities. The regulatory belief that these systems co-align to target ML is an oversimplification that undermines the intrinsic complexities within such systems. In this manner, and if we take a single organization as an example (say a financial institution), another need comes into being. The need to

> . . . differentiate between organizations themselves (for example the FATF, a central bank, a domestic bank) and the systems that emerge from the way these organizations operate. Each system is the totality of all that emerges from an organization's operations, and it is not restricted to a naïve description via an organizational chart and a collection of organizational documents (Angell and Demetis, 2005).

Beyond the organizational aspects, if one considers the system of technology, things become much more complicated as demonstrated by the variety of information systems affecting AML processes in the case of Drosia bank.

The interpenetration of systems within the domain of AML effectively means that no system is independent of other systems. Any given system at any given point in time is structurally coupled with a number of other systems with which it co-evolves. AML itself is structurally coupled with ML in a form of co-evolution that brings their interaction (AML and ML) within the sphere of self-reference and beyond the conventional ethical domain of good and evil. This means that by adopting systems theory, the common justification for the existence of AML that ML is a problem per se is bypassed by the systemic necessity of the system/environment difference; a system cannot exist without an environment. Such interpenetration, however, also implies confusion of purpose. This becomes widely observed in a variety of AML systems that wittingly or

unwittingly counteract the perceived goal of combating the phenomenon of money laundering. This is often because subsystems impose their own agendas that can often be contradictory to such a perceived goal, either because of increased complexity and the subsequent difficulty of controlling the outcomes of decision-making processes or simply because these outcomes generate unexpected positive feedback. Such positive feedback tends to destabilize the working processes of another stakeholder within the AML system, one that is supposed to share the same goal of targeting ML.

An example from the United Kingdom can be viewed as typical of such a phenomenon, where the introduction of AML technologies (imposed by the Financial Services Authority[1]), as well as compliance-fear and financial fines, generated a positive feedback that left the FIU of the UK in a state of denial, swamped with STRs and forced either to prioritize the reports or to put them on hold, unable to cope with their volume. A few years after the introduction of AML technologies, a backlog of STR processing of more than 8 to 10 months was experienced by the FIU (KPMG, 2003). By the time a suspicion was forwarded to a Law Enforcement Agency (LEA),[2] the money trail could have been rendered untraceable. This is typical of the explosive complexity that can be witnessed and one can only begin to imagine the organizational implications of such deficiencies or the decisions taken to bypass the problems.

Systemic considerations of such processes are never straightforward; the complex pattern of interactions that they require implies that such processes exist simultaneously at various subsystems. As these subsystems interact in both structured and unstructured ways, they participate in the generation of emergent phenomena that can only become visible a posteriori the interaction and never to their full extent. In other words, there are no cause-and-effect processes underpinning what we perceive to be the 'result' of those interactions.

As this constant interpenetration between systems, subsystems, and so on takes place, observers come along posing questions of the phenomena they observe. Then suddenly, systems acquire purpose and questions are derived by observations: questions that target the phenomena, questions that observers attempt to resolve with unique answers (for example whether something is true or false). But questions with a binary resolution (true/false) can never satisfy the demands posed by the systems theoretical stance. As Harold Pinter said on a rather remarkable Nobel prize acceptance speech, truth is forever elusive as 'there are no hard distinctions between what is real and what is unreal, nor between what is true and what is false. A thing is not necessarily either true or false; it can be both true and false' (Pinter, 2005). It all depends on the observer who is employing

his or her own operations of observations, and automatically leaves something unobserved (Luhmann, 2002), while recognizing that different observers can attempt different descriptions of any problem domain. On such occasions, success or failure become equally irrelevant. The success or failure of any AML stakeholder is but an isolated incident within the vast gulag of underpinning complexities with which they operate and/or they help generate. Philosophically, this requires the recognition that any function (such as success or failure of AML) is never an intrinsic characteristic of the object of study, the system that is being examined; it is always observer-relative and imposed (Searle, 1995).

If we are to ask about the properties of the AML-system and how it may be described in general systemic terms, then a first response might be attempted as follows: the AML-system can be described as a system of considerable complexity, structurally coupled with ML in the form of a co-evolution, and deviating considerably from what is commonly perceived to be a tidy demarcation of hierarchically structured organizations. However, as the systemic character of AML begins to unravel, it is clear that there is still a great deal to resolve.

What AML system? How does that 'AML-system' fit in with other systems and what are those systems? How are they constituted and how do they affect each other in the systemic sense? What is the most fundamental characteristic of an AML system? How do information systems come into the picture, and how do they affect the world of AML?

Following what has been discussed thus far in this first attempt to bring together some aspects of AML and systems theory, we will now delve deeper and ponder the fundamental questions outlined in the paragraph above. In order to do that, Luhmann's perspective on the functional differentiation of society will be used. Influences from information systems will be included in order to extend Luhmann's theoretical description by positioning technology within such a schema.

THE FUNCTIONAL DIFFERENTIATION OF SOCIETY AND THE ROLE OF AML

Anti-money laundering does not exist in a void. As already discussed, it is structurally coupled with money laundering and the two co-evolve in ways that surpass conventional descriptions of cause-and-effect. But there is another complementary way for describing the manner in which AML becomes co-dependent with other societal systems. Such a description can be found in what has become known as the *functional differentiation of society into subsystems of an autopoietic nature* (Luhmann, 1995, Moeller,

2006). As analysed in the systems theory chapter, autopoietic systems are systems that have the ability to make and re-make themselves by referring to their own functioning, and by utilizing their own elements.

The differentiation of society into its function-subsystems is informed by four essential assumptions:

1. There are *functions* that characterize the subsystems and become constitutive of the subsystems' internal operations. Functions are different from hierarchies in that functions always synthesize a multitude of possibilities within the subsystems, and become an alternative form for expressing unity and difference.
2. The system of *society* is considered to be the predominant system to which all others refer and into which all are incorporated; it is only the system of society that is operationally closed by the function of *communication*.
3. *Differentiations* within society are those that give rise to the constitution of subsystems within it. Such subsystems also communicate, as this is the primary function of the society within which they are embedded. Without communication at the subsystemic level, communication between the system and its environment becomes non-existent. This implies that positive feedback generated by the environment would enter the system and would ultimately threaten the system's survival. Prevention of such a destructive mechanism indicates that subsystems within society equip themselves with additional forms, norms and *codes* of communication that become a distinct set of characteristics of their functioning. In this sense, communication itself becomes differentiated within the formation of subsystems and two modes of communication can now be realized. One mode of communication is used within the subsystem and is utilized to communicate the function of the subsystem internally (amongst its own stakeholders/sub-subsystems in themselves). Another mode allows for communication between different subsystems of society like the political, the legal, or the economic.
4. Following functions, society and differentiation, *autopoiesis* becomes one of the most important characteristics within the functional differentiation of society into subsystems. Without autopoiesis the subsystems lose the ability to re-make themselves and reconstitute their elements, as they face the ambiguities of the environment with which they are coupled. Autopoietic systems are operatively closed and in this sense they are autonomous systems (Luhmann, 2005). A system in this sense cannot be more or less autopoietic; but it can be more or less complex (ibid).

With these initial comments regarding the functional differentiation of society into different subsystems, one can proceed into consolidating these aspects in a definition for such a differentiation. According to Luhmann, '"Differentiation" means the emergence of a particular subsystem of society by which the characteristics of system formation, especially autopoietic self-reproduction, self-organization, structural determination and, along with all these, operational closure itself are realized' (Luhmann, 2000b).

However, it needs to be made clear that such a differentiation of society into subsystems is not a process that occurs as a top-to-bottom imposition, but rather it is guided initially by particular inventions that generate the differentiation, and hence make the constitution of subsystems necessary. One can observe then that,

> Unlike in the ancient European description of society, such as Plato's theory of the politically ordered society (*politeia*, republic), this does not happen in the form of the division of a whole on the basis of essential differences between the parts. Indeed, differentiations in social evolution do not arise in this way, from above, as it were, but rather on the basis of very specific evolutionary achievements, such as the invention of coins, resulting in the differentiation of an economic system, or the invention of the concentration of power in political offices, resulting in the differentiation of a political system. In other words, what is needed is a productive differentiation which, in favourable conditions, leads to the emergence of systems to which the rest of society can only adapt (ibid).

Within such a description of functional differentiation of society, the question that arises almost immediately is how AML as a system can be positioned within society. Can it even be characterized as a system? One can begin to suspect that AML refers to the economic system and hence can be described as just another system within the system of economy, but that doesn't say much; even more importantly, as far as this book is concerned, the positioning of technology within *systems*, and how technology comes to affect the construction of the AML system remains elusive. Is technology a *system*, and if so, how? To attempt to resolve such issues, this book resorts to the crucial issue of *coding*, an issue that is at the heart of any distinction-making process within systems theory. In order to do that, it is important to examine the relations between the domain of AML and the attributes outlined above for autopoietic systems (function, differentiation and autopoiesis itself).

In this regard, the *system of AML* can only be characterized as a system if it is based on the attributes of function, differentiation and autopoiesis. Whether and to what extent different observers perceive, construct, and analyse a different AML system is one thing; but to deny the ontological presuppositions that give rise to the AML system itself, including the institutional fabric of the political, legal and economic systems (we call them

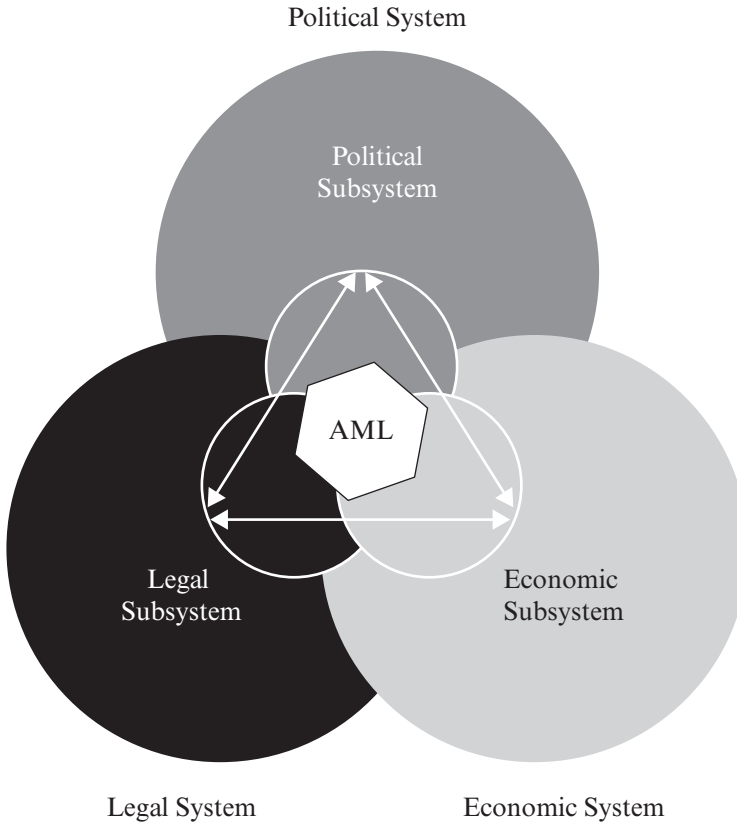

Figure 5.2 The functional differentiation of AML

function-systems) that support the institutional realm of AML, would be a grave mistake. It is interesting to note, however, that the manner in which this institutional support is given is self-referential and even more so, autopoietic!

All function-systems, the political, the legal, and the economic, constitute within themselves subsystems that refer to the projected function that a potential constitution of an AML system could attempt (targeting ML). By the communications and interactions between these subsystems, what emerges can be described as the perceived single entity that we may call the AML system. This is portrayed in Figure 5.2, a figure that strays away from the hierarchical mode of functioning depicted in Figure 5.1. The need for communication between the function-systems is essentially what destroys much of the hierarchy and linearity. Function-systems have their

own intrinsic complexity, but they allow for other function-systems to penetrate this complexity by means of communication; such communication becomes responsible for the emergence of new structures.

Even though, for the purpose of retaining analytic simplification, the predominant functional differentiation of the political, legal and economic systems describes these three as systems in themselves, that does not preclude the idea of them being subsystems within society. However, the subsystems indicated in Figure 5.2, refer to the constitution of subsystems *within* the political, the legal, and the economic systems. These subsystems express, by inter-communication, the systemic formation, constitution, representation, and sustainability of the AML system. Every system contributes in a different manner within the broader schema of the emergent AML system. Let us now examine how each function-system participates in AML.

The political system expresses the initial momentum based on the function that characterizes the political system itself, that of power. The legal system contributes by constituting the illegality of particular acts; it creates expressions that give rise to the ontological status of money laundering within the legal system itself. Ontologies can be drawn differently and hence it does not mean that the legal system defines what money laundering is. This is merely a delusion that will become more evident later on. Finally, the economic system contributes by providing those organizational structures where the applicability of AML laws and regulations can be realized and implemented (financial institutions for example). The use of subsystems at this level indicates that not all of the political, legal, or economic system is exercising its control for AML purposes. This does not mean that systemic interpenetration is absent; the possibility that other subsystems within any of the functionally-differentiated systems will be influenced by AML is not only present, but becomes unavoidable whenever a change within the AML system occurs. In this manner, different subsystems regroup and reorganize themselves for the production of a change; such a change may occur accidentally (perhaps triggered by the environment), or planned by the AML system that communicates its deficiencies to itself and to all other systems (political, legal, economic) within which it exists.

The AML system is neither static nor controllable in the cause-and-effect sense. This requires that the function-systems that come together for the emergence of the AML system cannot be static; the relations they develop keep being negotiated systemically and it is this re-negotiation that contributes to the self-referential evolution of the AML system itself. But this emergence of the wider international AML system from the major function-systems described above is something that was previously described to be self-referential. This requires further consideration.

Consider the political system, which refers to its own operations, and

hence is able to refer to its elements for the constitution of any subsystem within it. In this manner, it is self-referential, as are the legal and economic systems. By the ability of all these systems to refer to themselves (the primary concept of self-reference), they gain the capacity to carry out internal differentiations, and hence constitute other systems within themselves. In the particular scenario examined, it is such a subsystemic constitution that results in the emergence of an AML system. This systemic capacity underpinned by the concept of self-reference implies that an emergent system (for example the AML system) acquires the property of self-reference out of the systems that communicate for the act of its systemic formation. In this way, the newly established self-referential system (AML) participates in a broader process that not only re-creates self-reference out of self-reference, but in doing so, it also creates systems out of systems. Therefore the subsystems that come together for the emergence of the AML system harbour the possibility of uniquely determining the hypostasis of its self-reference, as the self-reference that characterizes them serves the function of generating autopoiesis out of autopoiesis when relating to systemic formation. What does this mean? And why is it important?

This autopoietic transcendence from one system to another implies that the autonomy of systems expressed through self-reference is passed on from other forms of functionally differentiated systems, which gifts the new systems with the property of autopoiesis. Systems equip the new systems with something that can solidify their autonomy and then systems merely compete with each other (and their environments) on the evolutionary advantages that they seek to gain from such interactivities.

So what is that 'something' that supports the autopoiesis of the AML system as described above? We have already seen how the AML system is differentiated within other systems of society, and how that differentiation helps to construct an emergent AML system. But differentiation itself is not enough; autopoiesis needs to be present as a systemic characteristic of the new system, otherwise without the ability to 'make itself' the system ceases to exist.

Thus the autopoiesis of the AML system comes into being out of the autopoiesis of the systems that generate it. This renders autopoiesis itself insufficient for sustaining any system by itself; a *function* is required that describes the specificity of what it is that any such system does. Of course, within the concept of autopoiesis we may find the general characteristics of self-organization and the re-arrangement of a system's elements and relations. Elements and relations come to be aligned and re-aligned in order to serve, or destroy, the function with which observers equip systems.

The concept of *function* therefore is absolutely central to the constitution of the AML system. But what is the particular function of the AML system?

Is it to combat ML? Clearly, that would be an understatement, given the structural coupling between the two. But what has been described thus far brings us to the realization that in any act of systemic formation (like the formation of the AML system), function, differentiation, and autopoiesis are equally important. They are created together. And in this event, as with any other system that comes into existence, there is something more that holds together all three primary concepts (function, differentiation, autopoiesis). That missing element is called the *code* of the system.

CODING

The issue of coding lies at the core of this chapter. It will serve as a step towards combining systems theory, the formation of AML, and the relationship between AML and technology as a set of interacting information systems. First of all there might be a terminological ambiguity that needs to be resolved. The issue of coding has got absolutely nothing to do with computer coding. The latter process if required is always termed 'computer programming', so as to avoid any confusion.

A code within a system has a primary utility: communication. Communication takes two distinct forms based on the code: the code serves (1) to facilitate communication between the subsystems of the system, and (2) to ensure that there is something that constitutes the fundamental difference being communicated from subsystem to subsystem in a self-referential fashion (hence maintaining and re-creating autopoiesis as described in Chapter 3). Regardless of the variety or complexity that subsystems may exhibit, they always have to refer to the code in one way or another. Each of these possibilities will be examined separately in order to make this point as clear as possible. For this purpose, the example of the legal system is used before turning to AML.

The code of the legal system for example is being determined inside the distinction of *legal/non-legal.* The code can only be established as the unity of the distinction between these two values (legal, non-legal) that are used in order to facilitate communication amongst all of the legal system's subsystems. This means that whatever subsystems may exist within the system of law, such subsystems always communicate within the constraints of, and by the use of, the fundamental distinction between legal/non-legal.

This distinction between legal/non-legal that serves as the code of the system of law, has considerable systemic implications, because

> . . . while the distinction between legal and illegal can be maintained for individual coding, the system as a unity can never decide the basis of what is legal or

Table 5.1 Codes and systems: fundamental unities of distinction

System	*Code*
Law	legal/illegal
Politics	government/opposition
Science	true/false
Religion	immanence/transcendence
Economy	payment/non-payment

> illegal. It can never apply the code to itself as a system. There is no foundational value establishing what is legal or illegal, only operations (Luhmann, 2004).

Therefore the code itself plays a fundamental role in the formation of a system. As the code characterizes the systemic function of differentiation, it is impossible for the system to use the code to describe itself. This means for example that the distinction being used 'enables the legal system to operate legally (!) by declaring that something is legal or against the law' (Luhmann, 2000a). The code exposed in this way becomes the first expression of self-reference within the system, and also the foundational representation of all autopoietic functioning without which the legal system would not be able to sustain itself, let alone become differentiated. Within five major functionally-differentiated systems of society, the code in respect to each system is portrayed in Table 5.1 (Moeller, 2006).[3]

The fact that the code cannot be applied by the system to itself is something that should place the concept of the code at the centrepiece of systemic formation (the act of formation of any system designated by an observer). If the system was able to apply the code that is constitutive of the system's differentiation, then that would mean that the system would be able to describe itself fully. However, that possibility of a system describing itself fully can only arise if the system uses its whole self for the description. That is tautological. It creates an entity with no connecting value, an entity that cannot be connected to any other. In recognizing the importance of this problem, Luhmann remarks the following:

> If one tries to observe both sides of the distinction one uses at the same time, one sees a paradox – that is to say, an entity without connective value. The different is the same, the same is different. So what? First of all, this means that all knowledge and all action have to be founded on paradoxes and not on principles; on the self-referential unity of the positive and the negative – that is, on an ontologically unqualifiable world. And if one splits the world into two marked and unmarked parts to be able to observe something, its unity becomes unobservable. The paradox is the visible indicator of invisibility. And

> since it represents the unity of the distinction required for the operation called observation, the operation itself remains invisible (Luhmann, 2002).

The above extract indicates that the code is not only a necessary paradox that cannot resolve itself (in being utilized by the system that incorporates it), but also a foundational aspect of the constitution of any system. Without this initial asymmetry exposed by the fact that the code cannot be defined by the system, the system would not have been able to expand itself or even to enable communication amongst its subsystems. The asymmetry induced by the introduction of the code within a system is a necessary prerequisite for the evolutionary steps the system will take in re-defining itself and exploiting its environment. In other words, asymmetry is a necessary prerequisite for self-reference.

Having dealt with the relationship between code and self-reference, it is now time to turn to the second most important role that the code helps to establish, that of communication between subsystems within the system. But that is not the only form of communication possible. The system, and any system, also communicates with its environment. If we again take the legal system as an example, then it becomes obvious that the legal system differentiates itself from other systems in society by referring to its code (legal/non-legal). Systemic interpenetration implies that the legal system influences other functionally-differentiated systems of society (such as the economic system) by 'transmitting' its code. The way in which this happens is through the depiction of the code into an instance of a notational schema that constitutes the means of communication, typically in the form of legal documents, articles, and so on.

But even within the legal system, the code serves as a mode of communication between subsystems of the system itself. The subsystems of the legal system also utilize the code legal/non-legal, as a means of both establishing and perceiving themselves as subsystems of the legal system (for example a law firm). In this way subsystems become autopoietic, and they also gain the means of communicating with other subsystems within the system. Hence, the code of any system plays a critical role in establishing the concept of the system and in facilitating communication within that system. The code is what penetrates all subsystems within a functionally differentiated system, and is what ties together function, differentiation and autopoiesis.

THE CODE OF THE AML SYSTEM

Making the utterance that there is such a thing as an 'AML system' means that this system displays all of the attributes discussed in Chapter 3 (such

as self-reference, emergence, complexity and entropic and negentropic effects), as well as those characteristics discussed above: function, differentiation, and autopoiesis. It also means that there is a code for the AML system with which the system is able to bring all these aspects together and hence differentiate itself, allow for communication amongst its subsystems (that is AML subsystems) and become autopoietic.

As the aspects of how AML differentiates itself and becomes autopoietic have already been analysed within the schema of the functional differentiation of society, what is essentially left is establishing the code of the AML system and describing how that code is applied within the system. As Luhmann notes regarding the applicability of the code and its relation to the system,

> Codes are abstract and universally applicable distinctions. Although formulated in terms of a distinction between a positive and a negative value, they contain no indication of which attribution is correct, the positive value or the negative one. Truth, for example, is no criterion for truth, and property is no criterion in the question of whether it is worthwhile acquiring or retaining it. It is only under the condition of openness towards both the positive and the negative condition that a social system can identify with a code. If this occurs, it means that the system recognizes as its own all operations that are guided by its own code – and rejects all others. The system and the code are then firmly coupled. The code is the form with which the system distinguishes itself from the environment and organizes its own operative closure (Luhmann, 1993).

In looking at what one might term an AML system in the systems theoretical sense and extrapolating from Luhmann's important remark, there is only one abstract and universally applicable distinction within AML that at the same time can be formed within both a positive and a negative value. That is the difference between suspicious/non-suspicious. Hence, for the AML system, the *code is the unity of the distinction between suspicious/non-suspicious.* The function of the AML system is to allow the communication of its code amongst its subsystems and between itself and its environment. This has further considerable implications on how the system itself enables communication amongst the subsystems within it.

From what has been discussed thus far regarding the issue of coding, we are now on track for elaborating the particular code for the AML system while examining various ways in which the code itself is influenced within the system of anti-money laundering. The unity of the distinction between suspicious/non-suspicious which constitutes the code is first of all associated with the constitution of the AML system itself and its emergence as a differentiated system within society. As an abstract yet universally applicable (within the system) distinction, the code becomes applicable to all different subsystems within the AML system. It does so by supporting

communication between the system's subsystems on the basis of what is suspicious/non-suspicious.

As with any other system that is designated by an observer, it is also the case with the system of AML that the code cannot be applied by the system to itself. Hence, applying Luhmann's remarks to the AML system, there is a need to acknowledge that there is no foundational value establishing what is suspicious/non-suspicious, there are only operations. This exposes the semantic problem of AML at its systemic core. It may be difficult to establish what is truly suspicious, but the operation takes place anyway otherwise the subsystemic functions are rendered redundant. Without this initial asymmetry, the subsystems of AML cannot communicate. They have to signal to other subsystems, and to the environment of the system to which they belong, that suspicious behaviour is communicated. But abandoning the other side of the distinction embodied in the code (/non-suspicious) is not possible; in fact, in all communication taking place within the AML system this does not occur. As 'truth is no criterion for truth and property is no criterion in the question of whether it is worthwhile acquiring or retaining it' (ibid), so it is with suspicion: suspicion is no criterion for determining whether something is suspicious or not. The code of the AML system, being the unity of the distinction between suspicious/non-suspicious, never ceases to exist within AML; both sides to the distinction created by the terms suspicious and non-suspicious must be maintained. This may temporarily create a contradiction and a question may emerge: how is it that when something is identified as suspicious that the non-suspicious side is not eliminated, but is instead maintained?

First of all, the unity of the distinction remains intact as one presupposes the other for communication. At the pragmatic level where AML stakeholders operate, communication implies that new stakeholders within AML will be called either (1) to reinstate the distinction and establish further the side of it that had been communicated (say suspicious) or (2) to reverse the distinction and maintain the other side (non-suspicious in this case). The complex operations that come together in order to determine (not causally) whether it is one or the other side of the distinction that is communicated are influenced by the different organizational structures and managerial circumstances within which AML individuals operate. These processes are also influenced by technology and the complex information and communication operations that technology supports.

How the unity of the distinction that constitutes the AML-code is preserved can perhaps become clearer with the following example. Let us suppose we are examining the process of monitoring transactions, where a particular staff-member of a financial institution identifies a

transaction to be suspicious. The method for communicating suspicion is encapsulated within an STR. The function of the STR is then to generate and communicate a temporary asymmetry between suspicious/non-suspicious, hypothetically abandoning the non-suspicious side of the distinction and communicating suspicion alone. However, identification of suspicion by one stakeholder within a financial institution neither negates the code, nor dissolves the distinction between suspicious/non-suspicious. What it does is merely to create a temporary asymmetry in the distinction. When another stakeholder (say an MLRO) receives an STR, he/she is called to re-realize the distinction between suspicious/non-suspicious. The MLRO in this case does become aware of the initial intentionality of a staff member to communicate suspicion, and by deciding to forward the STR further to the FIU, the suspicious/non-suspicious distinction is equipped with another asymmetry towards the suspicious side of the distinction. This self-referential spiral of the distinction between suspicion/non-suspicion can never be totally dissolved within the AML system. As long as communication amongst the subsystems of the AML system takes place, it is the asymmetry between suspicious/non-suspicious that is essentially reinforced. One of the two sides of the distinction is therefore strengthened while communication takes place within AML, but that communication does not negate the existence of the distinction itself. Until communication takes place between the AML system and the legal system, which will in turn operate by referring to its own code (legal/non-legal), ML prosecution cannot be justified. Even though the handling of the AML code within the AML system is indeed informed by what is legally defined to be money laundering (for example through particular designated typologies), the code suspicious/non-suspicious becomes constructed within the AML system. The variety of examples discussed within the case study of Drosia bank illustrate that this construction of the code suspicious/non-suspicious is supported by a number of complex (and often contradictory) processes. Even though it may be claimed that these processes are originally constructed by legislative stimuli (for example the legal system defines what processes are to take place and how potential ML should be handled), the interactions that they re-create become more impenetrable as their effects deepen. However, it is only the legal system, and in fact, the prosecution of an individual that can determine whether an act can be classified as money laundering (if individuals are eventually convicted and found guilty of ML).

With the introduction of the now infamous risk-based approach, which is supposed to provide an improvement in how the AML system handles its cases, the code plays a fundamental role in the construction of risk. If

we accept that risk is always implied in the construction of the distinction between the terms 'suspicious' and 'non-suspicious', we can observe how the communication of the distinction in the form of an STR, does not in fact collapse the distinction to its 'suspicious' part! In fact, and as noted in the sections above, the distinction between 'suspicious' and 'non-suspicious' has the potential of transcending different subsystems within the AML system. Technological support that automates the handling of suspicious transactions, compliance fear, as well as the issue of over-reporting are but a few elements that intensify the problem (Demetis and Angell, 2006). In the UK for example, as financial institutions and other stakeholders simply viewed the entire process as a 'tick in the box', they reported almost all possible suspicions under the fear of regulatory enforcement. Thereby, the risk was passed on to the FIU, whose staff could not be certain whether 'real suspicion' was being reported. They were therefore being forced into re-realizing the distinction between suspicious and non-suspicious, despite the fact that the STRs are supposed to communicate suspicion alone! The quality of the reports was therefore brought into question, and extra risk was introduced. The systemic implications of this need to be made clear: just because the distinction (suspicious/non-suspicious) collapses in the form of an STR, which is supposed to identify only suspicious transactions, that does not mean that the distinction has disappeared (Demetis and Angell, 2007). The distinction between suspicious/non-suspicious can re-surface again, and again, and again, and differently to every possible stakeholder operating within the AML system. The oversimplification, that STRs are there to indicate suspicion needs to be reconsidered; the preservation of the fundamental distinction between suspicious/non-suspicious has considerable implications for risk. Risk cannot therefore be specified or pointed out simply because it is categorized, even when the perception of risk is communicated; its re-genesis will transcend any system that attempts to manipulate it.

By viewing AML as a self-referential system with its code framed within the distinction suspicious/non-suspicious, it is important to realize that any systems-theoretical oriented research around AML must examine how the code of the system is affected by processes, operations, decisions, and so on. Academic research that establishes these effects is useful in many ways. It uncovers how the AML system operates and communicates the code internally; it assists in the description of those processes that construct suspicion/non-suspicion and it may provide some illumination on how the complexity surrounding AML can be effectively reduced. In the section that follows, an attempt is made to establish such descriptions between AML and the information systems discussed in the case study of the financial institution.

THE ROLE OF TECHNOLOGY IN THE AML SYSTEM

Before the role of technology is examined within the AML system, it is important first to ponder the question of the broader role of technology in modern society and then to reflect on what consequences technology has had on the AML system. As it has become obvious in the systemic theorizing carried out in this chapter, the AML system transcends all subsystems within which the code suspicious/non-suspicious can be communicated. While the majority of the empirical findings have come from the case study, and therefore justified inferences can be attempted within the realm of financial institutions, this does not mean that the role and influence of technology stops there. Technology does have an important impact on FIUs as well, but to be able to detail such an assertion one would be required to carry out further research on two different fronts. One would involve the incorporation of technology within the FIU itself and the consequences of utilizing different information systems for coping with the work in the FIU. Another would require an investigation of how the generated complexity from information systems comes to bear upon the broader national AML system (part of which is the FIU). In this latter case, an example is analysed further, based on data collected from the national FIU to which Drosia bank was submitting its STRs (see below).

One set of consequences has become evident in Chapter 4 through the in-depth case study of IS influences on AML work within the bank. In trying to expand these inferences and to examine the interplay between information systems and human activity systems (such as prosecution of money launderers) some further data has been gathered on one more instance that systemically affects the FIU and prosecution authorities, and for which technology at the level of financial institutions remains crucial. Needless to say that the process of juxtaposing data collected at FIU level with data regarding prosecution of money-launderers was a painstaking process due to access restrictions. Despite the small amount of data that could be collected for this purpose, the systemic results are crucial and complementary to this book.

In considering technology as a system within the realm of this structural yet constitutional difference between system and environment, a set of issues arises almost immediately. If technology is a system, then what is its environment? If technology is treated as a system within the schema of the functional differentiation of society, which has emerged in a bottom-to-top fashion from particular scientific breakthroughs (like the invention of the microchip), then in the environment of *technology as a system* would be other function-systems like the legal system, the financial system, the political system, or indeed subsystems of those systems like the AML

system. But in such a scenario wouldn't technology refer to those systems (say a computer-based system designed to operate for the financial system), and hence collapse to a subordinate *form* that loses much of its distinctive character? For reasons that will become visible almost immediately, the answer to this question is no.

Technology resists much of its subordination to a collapsed *form* of application by penetrating the core of other systems that attempt to manipulate it. Of course the systemic aspect of complexity analysed in systems theory could be alluded to here, or indeed, the law of unintended consequences that stems from such a complexity. But there is something more to the phenomena that technology helps generate.

Interpenetration of other systems with the system of technology implies a fundamental consideration that should not be underestimated. It implies that technology, with its distinctive character, *counteracts top-to-bottom processes of other systems that attempt to employ technology as form by generating bottom-to-top processes that display a unique set of properties and that elevate technology from form to system*. The concept of form in this regard implies a subordination of technology by stakeholders that adopt it for application in a particular problem domain. A clear example on technology *viewed as form* is the belief/delusion that we install technology in financial institutions in order to fix a problem or to handle a problem area (for example to combat ML). Contrary to form, the concept of system, when referring to technology, implies that technology retains all of its systemic attributes.

In order to use the core principles of second order cybernetics, the issues of observation and system need to be treated as intrinsically related. Defining any system must be, above all, an observer-relative act. Function-systems may of course be separated on the basis of purely analytical targets, but this in itself constitutes a form of simplification at the core of function-systems themselves; a paradox stemming from an observational simplification that makes observation possible in the first instance. The possibility for an artificial differentiation and separation of function-systems is somewhat countered by the concept of interpenetration and observation. This affects not only the systemic character of technology but also its *code*.

By departing from Luhmann's perspective on technology, one can expand the systemic treatise of systems (like AML) by treating technology as a system in itself. There is ample support for taking such a perspective based on the empirical data collected throughout the case study of the bank. Theorizing about the systemic nature of technology (and complementing it with further data), this book seeks a theoretical contribution at the level where technology systemically affects other systems.

Despite the theoretical rigour displayed in Luhmann's works, Luhmann has little to say about the role that technology has come to play in modern society and in affecting systems within it. Before the systemic properties of technology are examined by drawing from primary concepts of systems theory, like those of system/environment, observation, and self-reference, it would be prudent first to test Luhmann's perspective on technology, which is mostly depicted within his notion of *functional simplification* and *closure*. Resolution of the dilemma behind *form* and *system* cannot be dealt with without reflecting upon these concepts.

Functional simplification is a term that implies a reduction of an initial complexity that is subsequently streamlined within the realm of computer-based technologies. Closure implies 'the construction of a kind of protective cocoon that is placed around the selected causal sequences or processes to safeguard undesired interference and ensure their repeatable and reliable operation' (Kallinikos 2006). But to what extent does functional simplification and closure accurately describe the *Geist* of technology?

Here, it is claimed that functional simplification and closure remain considerably insufficient in describing the role of technology. The underlying assumptions behind functional simplification and closure imply that technology is subordinate to the initial reduction of complexity, devoid of any form of observational capacity. This does not agree with the theoretical stance developed in this book, and so an explanation will be provided straightaway.

Almost immediately, the above implication raises the question of whether machines can observe. This has to be treated differently in how observation operates within the realm of humans compared with that of machines. Inasmuch as observation is reflexively related to cognition, then machines can never observe, for they have neither the cognition nor the intelligence that comes with it. Intelligence in this regard is not logical, but biological (Angell, 1993). The evolution of such intelligence may very well be a product of both logical *and* biological operations, but never purely a logical one. It is the spontaneity in the generation of distinctions that ultimately guides observation and becomes the guiding factor in an emergent cognition (such as that of humanity). Since machines are restricted to carrying out simulations of logical operations, then how can they possibly observe, and why should we treat their so-called 'observation' as anything more than mere data collection, and a set of pre-programmed actions? It is precisely on the denial of this fundamental problem that Artificial Intelligence has struggled to keep its promise, albeit unsuccessfully. And this is exactly why the implementation of supposedly 'sophisticated' technologies for the targeting of ML have not lived up to the hype of their own

sophistication (projected of course by the software companies for profit-making purposes alone).

Nevertheless, there is one particular reason for assuming that technology does have some observational capacities, but only in the self-referential world of computation. This is because that world is one of excessive scale, information overload, and induced complexity that cannot be 'observed' by humanity, only by machine. This implies that technology becomes largely impenetrable; this is precisely what grants technology a systemic character that is much more complicated than what is captured by the notion of functional simplification. The fact that 'observation' by technology (say in the form of algorithms or a technology used in a financial institution for profiling ML) is devoid of all spontaneity and cognition does little to reduce the systemic character of technology itself.

The difference in how the term 'observation' comes to mean different things within the two distinct domains of man and machine can now be better articulated and considered: while humans possess a spontaneity in the generation of distinctions (though limited by sense-making restrictions and cultural biases), machines cannot spontaneously generate distinctions without a computational and engineered platform that will guide the process of generating distinctions. Computers may, of course, adjust, distort, manipulate the distinctions, but the rules for such adjusting, distorting, and manipulating (ultimately for data collection and *for a purpose*) are pre-engineered constructs.

Ultimately machines cannot think purposefully. Their non-cognition implies an 'Artificial un-Intelligence', and this is precisely their strength. Without non-cognition and un-intelligence, the machine operations that we now characterize as linear and automated would have been impossible. This is not to be taken as a patronizing assertion, or indeed as a celebration of the superiority of humankind. Humans view machines to be intelligent *because* machines are unintelligent. Machines thrive on linearity and automation. They streamline the logical predetermined paths that are pre-programmed to perform certain functions or operations. The inability of humans to perform large-scale automated operations quickly (say trillions of calculations) profoundly distorts our concept of intelligence, so that we believe machines can be eventually infused with a self-determined purpose. Consequently the mundane automation of tasks is elevated to something beyond mere processing.

Ironically, it is precisely this capacity for automation encapsulated by technology that creates its systemic character. Technology as a system can then be characterized by all the systemic attributes put forward in Chapter 3 and here. Technology as a system is above all a self-referential system. Technology refers to itself in two distinct and general ways. One

way involves technology influencing another technology (much like an information system in a financial institution influencing another information system within the same institution – this is supported by the majority of examples given in the Drosia bank case study). Another way involves connections between any technological artefact and itself, a self-referential system that evolves on the basis of information it receives from its environment. Interpenetration becomes evident between these two ways of technological self-reference.

An example here might help in clarifying this matter. Referring to a particular stakeholder (say a financial institution), technology as a system that influences the stakeholder essentially sets itself up in order to receive information of a particular type, such as financial transactions. Technology as a system then further structures this delimitation. Even more importantly, technology serves the function of automation, a function held together by the *systemic code of technology, the unity of the distinction between automation/non-automation.*

Systemically then, and based on the foundations of observation, the code of technology is no different than any other code. It is an abstract distinction and both sides to it are necessary. In other words, the very act of constructing an algorithm acts as an observation-act within the sphere of computing, thereby determining what is to be automated, and what is – at the same time – left un-automated. In constituting a system then, and much like observation that automatically implies non-observation of something else, the very act of constructing a technology implies that what is determined to be automated within the realm of a single technological artefact, immediately leaves non-automated elements that become constitutive of technology itself. Without such selection imposed by automation, the initial reduction of complexity would have been impossible.

As nothing can be considered in splendid isolation, technology too cannot be seen as systemically removed from the other systems that incorporate it, or outside of the multiplicity of interactions that it fosters. As it has become evident from the empirical findings, when different information systems interfere with each other, the process of reflecting upon the distinction between automation/non-automation becomes complicated but illuminating nevertheless. In the case of Drosia bank, this process is revealed by the exposition of the POSEIDON information system that still is the most central information system in day-to-day operations.

In the case of POSEIDON, it becomes evident that systemically, all problems start with an assumed unity (or rather the delusion of a perceived singularity). A false impression may initially be given that POSEIDON constitutes a single information system with neatly categorized informational consequences. However, in the research carried out in Drosia

bank, it has become evident that underneath the presumed unity of the POSEIDON information system lies a much more complex picture that cannot be easily decomposed or even fully resolved to the benefit of the organization itself. In this example, analysed fully in Chapter 4, it became evident that the underlying complexity of informational requirements and restrictions that created POSEIDON came from a variety of other 'singularities'; other information systems with other targets, scope and applicability. Examples in those systems that influenced POSEIDON included: card-data that were fed into the new system; previous legacy systems in different formats; interactions by staff members with POSEIDON that fed the system with multiple unique-identifiers of customers and wrong transacting codes.

Thus, information systems and their interaction play an important role in shaping the unity of the distinction between automation/non-automation. As each information system operated with its own set of rules for dealing with this distinction (rules that were affected considerably by designer choices, the needs of the financial institution, and technological and regulatory evolution), interpenetration – or actually forced interpenetration for centralization purposes that ended up in what is now known as POSEIDON – brought out precisely this distinction between automation/non-automation.

Along with the introduction of POSEIDON, new needs were therefore developed. As a new technology came along to serve new needs, it became almost inevitable that information elements, which were not considered in previous systems (and were hence left non-automated), had to be considered in light of POSEIDON. However, these non-automated information elements were structurally coupled with those that were automated, and further structured in a particular format. This observed interpenetration between old and new information items, which was reconstructed as a necessity during the creation of POSEIDON, created a variety of further problems. The starkest of all problems coming with the existence of POSEIDON was that of multiple unique identification numbers for a large number of customers, a problem that was effectively countering the original purpose for constructing this particular technological system!

From a purely operational perspective, none of this affected the customers of the financial institution as there were no implications for their banking transactions. The system had to be fully operational or otherwise daily business would have been non-existent. However, the emergent problems that came with the introduction of POSEIDON did create a number of difficulties for the money laundering analysis team. These ranged from establishing identity to investigating customers' total financial positions and transactions. On a number of occasions, AML investigations that

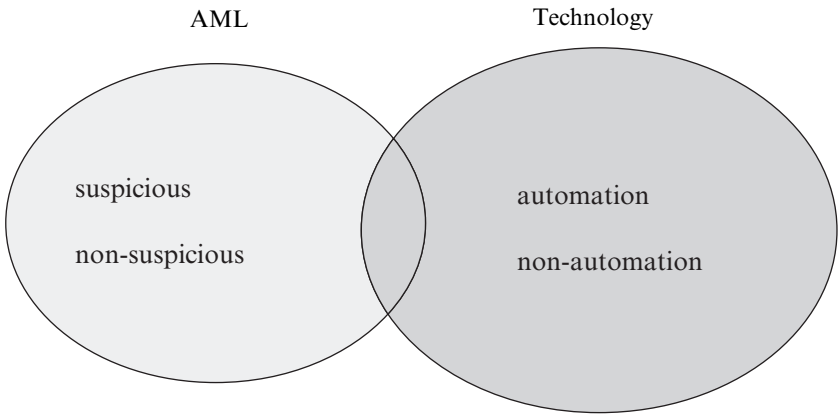

Figure 5.3 Interpenetration between the systems of AML and technology

were already time consuming became even more problematic. This led to the utilization of other information systems (like the FTEM analysed in Chapter 4). Complexity of a newly established informational base grew out of the complexity of a pre-established one.

With this example in mind, and the myriad other examples coming from the study of Drosia bank, it becomes evident that the concepts of functional simplification and closure remain insufficient for capturing the systemic dynamics of technology. Technology becomes a system in itself and retains a distinct systemic character that considerably affects the context within which it is embedded. The relationship then between the two systems of interest here, namely that of anti-money laundering and technology, can be framed on the basis of the *coding interactions*, as portrayed in Figure 5.3 above.

The consequences of such interpenetration become evident on the basis of the two unities of distinctions that are framed for each system respectively. For the AML system, the major distinction that is communicated is the distinction between suspicious/non-suspicious, while for the system of technology it is that between automation/non-automation. Linear analogies should be avoided here. This means that a direct relationship between what is technologically automated and utilized by the AML system, does not immediately relate to suspicion. The same analogy can be drawn between non-suspicion and non-automation. Not only does the possibility arise that both suspicions may be left non-automated, and non-suspicion automated, but also that this possibility is in fact a necessary precondition for the interpenetration of the two systems. Both sides of the distinction to each respective systems (AML and technology) are always present.

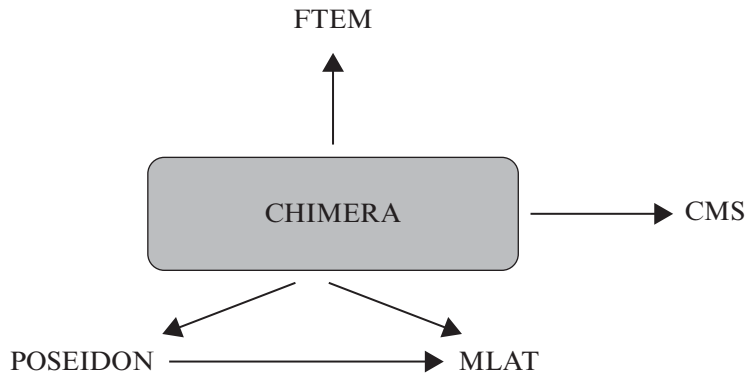

Figure 5.4 CHIMERA influences

In the example of the CHIMERA system, which became the first automated system to consider some filtering on the basis of lists like OFAC, CFSP and so on, and thereby to determine suspicion, the seemingly simple differentiation on the basis of the unity between suspicion/non-suspicion quickly generated complexity for other information systems that were affected by the introduction of CHIMERA (as shown in Figure 5.4 above), or that were affected by CHIMERA itself. A variety of other issues directly or indirectly affected the CHIMERA system. The SWIFT messages service problem analysed as an example in the case study (by pointing to the exclusion of keywords) was such an issue, only to be followed by language conversion issues, and a variety of complex patterns of interactions between AML and technology. Furthermore, shortly after the implementation of CHIMERA, it was realized that the Case Management System where STRs from the branch network are recorded, also required the input of names of suspected persons, names that were aggregated into widely available lists.[4] Duplication of manual inputting of the names on those lists of suspects became unavoidable, and another layer of complexity was added for the MLAT to deal with. The obvious overlap with the FTEM system was also deemed to be problematic, however as a variety of typologies were not covered in POSEIDON, problems in the simultaneous operation of the two systems became unavoidable.

One can observe that with the introduction of yet another information system relating to AML, the systemic emergent complexity increases considerably. This is in no small part due to the considerable interactions and interdependencies that any given system generates. This emergent complexity, however, also stands as an opportunity to ponder the broader effects that technology has in the AML-system.

Within Drosia bank a small part of this influence was demonstrated in the skyrocketing of the number of suspicious transaction reports year after year. Beyond the increased vigilance and training that staff members of the bank have had, one cannot but include technology as systemically organizing the increase of suspicious transaction reports for a number of reasons. For example, CHIMERA had a direct influence on a number of other information systems and orchestrated part of the increase. The ZEUS profiling system had a tremendous effect on the daily STR backlog with over 2000 suspicious reports per day. Long before that, the FTEM system communicated possibilities for suspicious names that could be further investigated at branch level, while at the same time serving as a reminder of the need for AML vigilance.

This increase in the number of suspicious transaction reports within the bank being examined is of course something that has alarmed the compliance officer and the management of the money laundering analysis team. To deal with this problem, as was previously noted, additional resources have been requested, and the MLAT has nearly doubled in size within a period of two years. By the end of 2009, the MLAT had quadrupled in size.

However, in taking a closer look at this problem of STR growth, an additional question was raised along the lines of the core research interests of this book and for which further data were sought at a national level. The question had two important parts. Is the increase witnessed internally in this single financial institution, typical of the whole banking sector? Has the number of STRs increased overall at the receiving end (the FIU) if we take the totality of the banking sector, and if yes, what have been the corresponding prosecution rates?

AML – 'ISLANDS OF REDUCED COMPLEXITY'

In attempting to answer these two further questions, and to reflect on this particular systemic aspect, relevant data were sought from the authority that was responsible and involved in both AML and prosecution. The data therefore that needed to be collected involved both:

1. Aggregate data on the *total number of STRs* received by the FIU per year. The STRs in this case came from the totality of financial institutions that submitted their STRs to the FIU. The data was in aggregate-form and therefore it was not possible to discover how many STRs came from specific and identifiable financial institutions.
2. Aggregate data on the *total number of prosecutions* for ML per year.

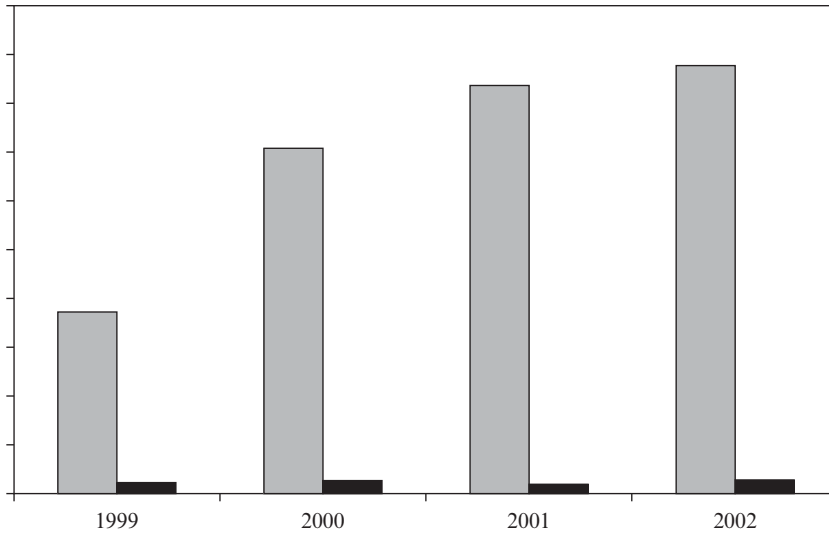

Figure 5.5 Disclosures/prosecutions for the national AML system

Two issues that restricted a deeper line of inquiry emerged. First, due to access restrictions it was not possible to aggregate the information regarding conviction rates in ML cases being prosecuted. Second, the period for which aggregate data were provided on both data sources referred to the 4-year period from 1999 to 2002. While it was not possible to retrieve further data on this matter, recent talks with the FIU (December 2009), confirmed that the data for this period remain representative of the national AML system for the period between 2002 and 2009.

Figure 5.5 presents the consolidation of these two sources that were disclosed to the author. The left-sided columns that depict a year-after-year increase, represent the number of disclosures to the national FIU in the form of STRs (submitted by all the financial institutions in the country), while the right-sided columns represent the number of prosecutions for each corresponding year.

Latest data (based on a communication between the author and the FIU in December 2009) have confirmed that while the number of prosecutions has remained similar, the number of STRs has increased another 300 per cent from 2002 to 2009. Evidently, one cannot but observe in Figure 5.5 that while the number of suspicious transaction reports was increasing year after year, the number of prosecutions remained nearly static.

A series of important considerations can be attempted in light of this finding and systems theory can once again bring this observation into

some perspective through what was analysed in Chapter 4, namely the concept of systems as 'islands of reduced complexity'. In order to evoke this concept and apply it in the particular circumstance, we require a differentiation between two further subsystems within the totality of the AML system (systems in themselves however). Since systems are observer-relative entities, we can further create the difference between the *system of generating AML-cases* and the *system of prosecuting ML-cases.* In this case, both systems would themselves be 'islands of reduced complexity' with one affecting the other. The major difference between the two systems, however, lies precisely in the possibility of technological incorporation that manifests itself, once more, through the distinction between automation/non-automation. While the system of generating AML-cases mostly refers to financial institutions that submit their STRs to the FIU and that are heavily influenced by a number of technological implementations, the system of ML-prosecutions unavoidably rests on manual processes. In effect, the system of ML-prosecutions can be characterized as a human-activity system that re-examines the code-distinction of the legal system (that being the difference between legal/illegal) in order to determine whether to proceed with a prosecution or not.

As a human activity system, the legal system faces a restriction that is not present in the system of AML-cases: its capacity for information processing is further limited by the manual processes that are a prerequisite for the system's own functioning and constitution. This creates another reduction of complexity that is not to be underestimated. First, the system is limited in itself as an 'island of reduced complexity' the moment it is identified as a system by any one observer studying it. Second, another reduction of complexity is imposed by the system with which it is structurally coupled (for example in this case that would be the system of generating AML-cases). This imposition of a further reduction of complexity is carried out by reframing the code-distinction between automation/non-automation. While the system of generating AML-cases activates the distinction between automation/non-automation by incorporating technology, for the system that is attempting prosecution of ML-cases the distinction between automation/non-automation is only a background.

Systemically then, this implies that the system of generating AML-cases, with the possibility of incorporating technology and utilizing the distinction between automation/non-automation, affects the system of ML-prosecutions, which is acting on its own code (prosecution/non-prosecution). With the information processing capacity of the latter system in mind, *the volume of submitted STRs remains practically irrelevant for the system's restricted capacity to prosecute ML-cases*! As an island of reduced complexity itself, and even further, one facing a double-reduction

in complexity, the system of ML-prosecutions faces a greater problem. Systemically, not only is one forced to admit that this reduction of complexity constitutes a necessary systemic prerequisite to the very act of defining a system, but that the mode of functioning of the system itself is influenced by the mode with which other systems treat their own complexity generation (and reduction!). Amongst an increasing white noise that is therefore being generated by the system of AML cases where financial institutions submit their STRs, the system of ML-prosecutions finds it even harder to operate. It must be pointed out here that the author finds it at very least ironic that some FIUs (for example AUSTRAC[5]) proudly proclaim an increase in the volume of STRs as if such an increase in itself constitutes a measure of the effectiveness of their national AML system. It is interesting here to note that in Australia, 10.7 million STRs in the year 2005 led to 1743 investigations (not prosecutions), a mere 0.016 per cent of the total number of reports, the same percentage as for 2002–2003. In previous years this was at 0.02 per cent for 2001–2002 and 0.009 per cent for 2000–2001, namely roughly the same insignificant order of magnitude. In Japan, to bring up another example, 98 935 STRs led to only 18 prosecutions.[6] Even though an empirical justification of the principle of reduced complexity would require a mammoth data collection worldwide (to juxtapose in every country the number of generated STRs to the number of prosecutions), it is in the author's conviction that further data would support the principle and the assertions underpinning it.

Exploring this dynamic behind the interaction of generated STRs and prosecutions raises the potential of reflecting further on the systemic nature of both technology and its interaction with AML. Through the primacy of the concept of 'observation' this first points towards the aspect that the designation of an entity like 'the totality of the AML system' becomes paradoxical for analytical purposes. The somewhat fashionable term that the world of AML has adopted, that of a 'holistic' approach in AML, is therefore misguided. The 'whole' can only be identified by exclusion of something else; no observation within that hypothetical 'totality' can take place without another internal differentiation that would re-assimilate the difference between system/environment. This may apparently create a series of problems, but one way to reframe this is by asking: once the AML system has been identified as the system to be studied, what potential internal differentiations can a researcher attempt in order to observe instances of AML subsystems, and where possible, to generalize these instances into properties of the system itself as emergent phenomena?

Following on from the role that technology comes to play in AML, in the example exploring the relationship between the number of STRs received in the national context examined and the number of prosecutions,

it becomes evident that the description developed in Chapter 3, where systems were seen as 'islands of reduced complexity', can be seen differently and expanded to include technological effects. Technology reconstructs the initial reduction of complexity that comes with defining a system as an 'island of reduced complexity'. While aspects of reduced complexity within the technological realm can be hinted at with Luhmann's concepts of functional simplification, they do remain insufficient once interactivities between systems are further taken into account.

This implies that the interaction between systems of technology and human activity systems can generate considerable asymmetries in the handling of a problem domain like ML. Technology for example, through the application of its code on automation/non-automation and its interaction with AML, comes to reduce the complexity of the system that it is supposed to counteract (that is ML). Through profiling software, case management systems, data mining platforms and behavioural modelling exercises among other things, technology automates aspects of ML modelling and of course, simultaneously leaves other aspects non-automated.

The increase of STRs prevalent within a number of different national AML systems worldwide, and supported to a large degree by technological implementations at various levels, becomes a background of white noise to other subsystems that have limited information processing capacities (through their own modes of reduced complexity). At the same time, technological implementations generate an increasing complexity within which other subsystems operate. Hence, an increase in STRs, supported by technology, introduces more and more white noise, more and more complexity, and within the generation of such a complexity, other subsystems (like prosecution authorities relating to ML cases) find it hard to cope with an information overload that they either have to ignore (because of their own modus operandi in dealing with complexity), or must attempt to reduce further in a number of ways that does not affect their own processing capacity.

THE TECHNOLOGICAL CONSTRUCTION OF AML-REALITY

In modern philosophy, a very important stream of thought that deals with social constructions has been advanced by John Searle (amongst others) in what is known as the *social construction of reality* (Searle, 1995). This implies that humankind and organizing societies come to refer to a reality (the environment of their system) that is socially constructed; essentially what is experienced is rendered into reality by interaction between systems

and their environments. Following from the treatise of technology as a system in its own right, it is argued here that reality is technologically constructed by means of interpenetration, where the code of technology (automation/non-automation) affects other systems. It is important to stress here that this viewpoint is considerably different from the general hypothesis researchers make while examining the effects of technology in various problem domains like anti-money laundering. However, before generalizing this assertion for all systems, the example of the AML system is used to outline how it becomes technologically constructed and how such a process differs from the common viewpoint that technology has come to occupy in AML-stakeholders (such as typically a financial institution incorporating technological artefacts for targeting money laundering).

Current anti-money laundering practices generally place information systems in a number of ways within the AML system, but the underlying assumption behind most of these implementations is that technology is a tool with which ML can be targeted. Extrapolating from chapter 4 and the instances of technology being used (POSEIDON, CHIMERA, Electronic Updates Systems, FTEM, Case Management System, ZEUS profiling software, and so on), information systems can be classified into the following categories:

1. Information systems that target money laundering explicitly (such as the ZEUS or the CHIMERA systems) or used for AML purposes (such as the CMS in Drosia bank). Such information systems are typically integrated within transacting systems of stakeholders that may be affected by money laundering, and they aim at preventing ML taking place (for example blocking a transaction from a person who is on the OFAC list) and/or simulating money laundering behaviour in order to flag up suspicious transactions for further scrutiny. Technologies that may participate in such information systems can be profiling, data mining technologies and the like.
2. Information systems that affect money laundering processes within financial institutions and/or other stakeholders, where the purpose behind their design was originally irrelevant to AML per se (the POSEIDON system and the FTEM system can serve as two such examples).

While research usually focuses on the first instance, and tries to establish causal links in demonstrating how technology targets ML, through the case of Drosia bank it becomes evident that there exists a much more complex infrastructure of information systems. Such information systems are prone to a degree of interdependency that makes it difficult to establish

a causal link between how one information system influences ML and how that information system is subjected to influences from other information systems or human activity systems. The interdependencies created and the complexity they help generate, re-construct the idea that technology is a subordinate form that is employed by financial institutions or other stakeholders to target ML. In orchestrating the emergent complexity of such interdependencies, technology becomes a system in itself; and in doing so, beyond the realm of the social construction of AML as an ideal (via the socially constructed idea of money as analysed in Chapter 2), technology constructs the reality of anti-money laundering by creating bottom-to-top processes that often counteract top-to-bottom designations of how AML should function.

By referring again to Figure 5.1 in order to indicate how perceptions of AML come to be constructed and how technology enters the picture, the following comments can be offered. From a stakeholder operating at the transnational level, say the EU, money laundering is defined in a well-structured manner, and such definitions are communicated to the stakeholders operating at both national and local levels. This communication does of course little to resolve the semantic issue of determining suspicion, but, as has been previously analysed, this is due in no small part to the unavoidability of collapsing the code of the AML system to only one part of the distinction between suspicion/non-suspicion.

In looking beyond the oversimplification, which both determines AML/ML through legislative initiatives and generates the impression that their structural coupling is under some stringent causal control, one can find that the 'reality of AML' is constructed through a multiplicity of complex interactions. Not that there is such a thing as one AML reality; one would have to neglect the existence of observers and their role in defining reality in the first place.

The point to emphasize here should be that the near total disregard for bottom-to-top processes, which become in many ways constitutive of a phenomenon being studied, create dynamics that restrict alternative perspectives. For the case of technology this appears to be particularly of interest as in a large number of fields, society has come to rely on the ceaseless and uninterrupted functioning of technology and has increasingly developed its own structures on the basis of this precondition. But once the consequences of this precondition appear not to be working and technology propagates systemically adverse effects within other systems, then surprisingly it is not the precondition (of uninterrupted functioning) that is put into question. A system then (the AML system, for instance) re-organizes itself in order to interpenetrate more with the system of technology, and hence subjects itself further to the distinction of automation/

non-automation without questioning either the precondition or the actual pragmatic effect of technology. This is precisely why every regulatory intervention for the introduction of AML technology at various national settings, has created a number of adverse effects for financial institutions, FIUs and prosecution authorities alike. When it comes to examining the incorporation of technology within the AML system and the emergent systemic character of technology, it appears that the precondition of technological functioning creates far more complexities than expected.

What the word 'technology' comes to mean in this context is another oversimplification that needs to be pondered further, and this has been one of the main goals of this book. Whereas technology for AML as commonly perceived would refer to only those technological artefacts that attempt to simulate ML behaviour for capturing suspicious transactions, one may observe that, by treating technology as a system in its own right, analytical differentiation within the system of technology may begin. Such an internal differentiation considers technology as a system with an environment, and of course, as a system with subsystems. Furthermore, if AML technology is treated as a system, then the subsystems may relate to different technologies that do not have to relate directly to the task of identifying suspicion. These subsystems can however be considered in relation to AML, insofar as they systemically affect the constitution of the problem domain, and most of all, the construction of its suspicious/non-suspicious code.

In this manner, as it became evident within the scope of Chapter 4 on the empirical findings, what we can refer to as *a system of technology affecting AML* is of considerably broader scope than technologies that attempt to simulate suspicious transactions. Beneath the complex interactive patterns of different information systems, the systemic code of technology based upon automation/non-automation comes to construct and reconstruct the fundamental systemic code of AML (suspicious/non-suspicious).

In this way, what we term technology is the unity of the various technological-subsystems (CMS, CHIMERA, POSEIDON, FTEM, ZEUS). Each of these technological-subsystems may in turn be perceived as an observing system in itself that incorporates the unity of the distinction between automation/non-automation. Therefore every technological subsystem is acting as a system in itself. Technological subsystem upon technological subsystem, automation upon automation (but also, non-automation upon non-automation), construct a complex array of variable interactions that come to define the methods through which the distinction between suspicious/non-suspicious is to be realized, thereby defining an important part of the AML system. In other words, and what has already been alluded to in the heading of this section, one may speak of the *technological construction of AML-reality.*

The technological construction of AML-reality implies that within the duality of the systemic codes of technology and AML, bottom-to-top processes that arise from complex interactions come to counteract top-to-bottom designations of how AML should function. In other words, technology and the complex interactions it engulfs when a variety of technological subsystems are examined for the purposes of AML-relations, acts as an entity defining AML, thereby propagating to the environment of ML.

If such is the technological complexity encapsulated within the realm of a single financial institution like that of Drosia bank then it is difficult for one to grasp conceptually the underlying technological complexity in all the financial institutions at a national level, each with its own evolution, organizational structure, procedural resolutions of system/environment conflicts, and ultimately, operative closures. This complexity remains hidden to a large degree by the further necessary reduction in complexity posed by communication between stakeholders. Thus, the communication between financial institutions and FIUs appears to be collapsing in the form of a singularity (that of an STR) while much of the underlying complexity orchestrating the suspicious/non-suspicious code for AML remains hidden.

Beyond the conventional realm of suspicion, therefore, a suspicious transaction report not only fulfils the function of communication by creating a temporal asymmetry between suspicion/non-suspicion, but also its very existence serves the systemic function of cutting down on the underlying complexity so that communication can be facilitated in a highly structured manner. The complexity that is collapsing into the form of an STR remains hidden. It remains hidden by necessity, for otherwise the FIU would suffer an immense information overload; ironically the FIUs nevertheless suffer information overload even in the simplified forms of STRs. Combining intelligence and informing LEAs remains no easy task when one intelligence agency has to act as a collection point for financial institutions (and other stakeholders at a national level).

In exposing the underlying complexity within a single financial institution, whether technologically supported or not, there is a number of benefits to be considered in the broader AML system. These include the FIUs, so that feedback mechanisms would reduce the white noise in the hope of a more effective communication of suspicion. However, the technological infrastructure through which suspicion is reconstructed remains highly complex. In fact, it becomes so complex that it acquires characteristics similar to those of a bureaucracy. The penetration of technology within modern institutions, not only reconstructs the bureaucracy within which they operate, but also develops a distinct character of its own. This has previously been designated by the author with the concept of *electreaucracy*, in order to denote the interference of technology in traditional

organizational structures by the systemic influence of the automation/non-automation code (Demetis, 2009).

THE SYSTEM OF TECHNOLOGY

As it has already been discussed, Luhmann's theory describes technology by means of functional simplification and closure. Devoid of general systemic properties on technology, Luhmann's theory does not examine *technology as system*, and hence the systemic effects of technology are underplayed by technology's perceived supportive role. Technology is hence seen as subordinate to other systems. In this book, both the empirical evidence as well as the theoretical development of systems theory outline a picture of complexity where the technological realm exhibits all the systemic properties of interest (for example self-reference, code, and so on). It becomes evident that *technology as system* creates emergent phenomena that counteract top-to-bottom processes by other systems (such as the legal system). In countering such top-to-bottom processes, a more complex structure emerges at the level where information becomes treated in an automated manner. The explosive complexity of IS-interactions in the case of Drosia bank is a testament to this. By treating technology as a system, and by examining the systemic effects and circumstances that technology comes to construct as it becomes structurally coupled with other problem domains, deep-seated effects are revealed that must be taken into consideration.

The very application of systems theoretical ideas on the problem domain of anti-money laundering introduces a series of important considerations. Even though this application of systems theory also involves a practical contribution, if one looks at this matter from a purely theoretical standpoint, it does readily demonstrate the theoretical diversification of systems theory and the theory's potential for analysing complex problem domains like AML. Beyond the realm of description, where every stakeholder within AML talks about some sort of vague 'AML system' and hypothesizes on the effects that various external or internal elements have on that system, systems theory allows for a discussion on what specific properties can be considered within the system, and why they are important. On a theoretical level it provides the AML domain with a description of its systemic characteristics that becomes invaluable when considering a variety of implications within that domain, be they technological or not.

Having discussed the interaction between information systems and anti-money laundering, this book will now discuss the risk-based approach and offer reflections on its application.

6. The risk-based approach and a risk-based data-mining application[1]

The introduction of the risk-based approach has undoubtedly been one of the most important regulatory steps that have been taken for the improvement of AML. In this final chapter, a deconstruction of the risk-based approach is provided and it is related to the text of the European Union's 3rd AML Directive (EU 2005). The deconstruction method uses systems theoretical ideas and Luhmann's application of systems theory on risk. Other key systems theoretical concepts are also used from the descriptions provided in the previous chapters.

Before considering risk in the context of AML, it is important first to reflect on both the nature of risk itself and the way it is observed. With risk being an important concept that is used in the vast majority of financial and other institutions, it is vital that the widespread misunderstanding in the way risk is perceived, represented and handled is exposed.

DECONSTRUCTING RISK

Risk is a subtle and elusive entity. Any representation of risk, and hence any attempt to break up risk into sub-categories, as in the so-called risk-based approach, requires the active involvement of an observer.

Two broad types of risk can be practically distinguished, namely (i) 'taking a risk', where an action is taken in search of opportunities, but with the possibility of facing hazards, and (ii) 'being at risk', where outside forces threaten. In both cases there is a fundamental problem: by necessity the observer must start in a state of uncertainty, before becoming aware of the risk. There is no need to distinguish between risk itself and the awareness of risk, since a lack of awareness will be subsumed back in uncertainty. The observer perceives the situation and then introduces some form of intellectual structure that mediates and transforms the vagueness of the uncertainty into risk. Risk is something that is capable of being represented; uncertainty on the other hand is a state of mind that is unknown and unknowable. By finding a way to represent risk our hopelessness with uncertainty is swapped for the optimism in a structured plan of action that

is meant to handle the risk. In other words, we impose some sort of structure in order to gain a tenuous handle on uncertainty, but in doing so we create other uncertainties.

Different ages have different approaches to uncertainty; different social, cultural, organizational and technological structures, each delivering different notions of risk, different categories of risk, and different risk assessments. The risk-based approach promoted in the 3rd AML Directive is just one of today's prevalent structures. The reason why the approach feels reasonable to us isn't that it is intrinsically valid, merely that it reflects the way we normally do things nowadays. And we do things that way because we believe that by doing so the uncertainty will dissipate, not be disruptive, and the outcome will be beneficial, or at least neutral. With the concepts of 'risk' and 'risk management' infiltrating every modern socio-economic and political institution, this is hardly any surprise.

However, in all this manoeuvring, we can easily forget the starting point: the problem of the original uncertainty and the form of the intellectual structure that was used to formulate the risk. This has to be addressed before we can even talk about risk, and before we can consider a risk-based approach. Clearly the role of the observer is absolutely critical here, both in the original formulation of risk, and in the creation of plans of action. Here it is worth quoting an extract from Niklas Luhmann's book entitled 'Theories of Distinction' on this issue:

> When observers (we, at the moment) continue to look for an ultimate reality, a concluding formula, a final identity, they will find the paradox. Such a paradox is not simply a logical contradiction (*A is non-A*) but a foundational statement: The world is observable *because* it is unobservable. Nothing can be observed (not even the 'nothing') without drawing a distinction, but this operation remains indistinguishable. It can be distinguished, but only by another operation. Or to say it in Derrida's style, the condition of its possibility is its impossibility (Luhmann, 2002).

The two apparently nonsensical statements, 'the world is observable *because* it is unobservable' and 'the condition of its possibility is its impossibility', actually make perfect sense. What Luhmann is saying is that observation is not, cannot be, what we think it is. Observation of a part, and hence the designation of a category, is only possible because the whole is unobservable. Not that the 'whole' in this respect can be defined, for then that 'whole' would need to be distinguished from everything but the 'whole' itself; that is distinguished from nothingness. The act of observation, therefore, necessarily actively involves the observer in the world, so that he has choices and is not at the mercy of inertia. That very act implies that the separation between what can be observed and what must be left

unobserved is more of a necessity than a mere compromise. Such a necessity however comes with problems and paradoxes: what is observed is not the thing itself, but an internalized representation of that thing, which has to fit into a category created for it by observation. The categorization of 'things' observed in the world is both the result of observation, and the means whereby observation is possible.

It is an error to insist that a categorical representation of a thing is identical to the thing-in-itself. Furthermore, treating the 'rest' as a separate 'residual category' is as much an error. It is an error that implies the systemic structural couplings between system and environment have simply disappeared; an error because then the two parts no longer comprise the original 'whole'. Thus observation, by its very nature, must introduce an asymmetry: the structural couplings are made to disappear from any representation of the observation, but they are still there in the world. They constitute a non-linear phenomenon both in the thing-in-itself and the unobserved remainder. The two artificially separated parts continue to operate (and interrelate) as the unobservable whole. Because of this asymmetry (between the world as it is, and as it is observed), observation is conditional, but those conditions are necessarily unobservable and unappreciable.

But observe we do. We continuously observe the paradoxical residual categories of previous observations, and in doing so, introduce new couplings among our ever-expanding set of artificially introduced observational constructs. Piling them up, memory upon memory, paradox upon paradox, uncertainty upon uncertainty, all thought of the fundamental asymmetries is conveniently ignored in our tidy descriptions. Thus, we delude ourselves that through observation we 'understand' risk in the 'real world.' However, those truncated structural couplings, so casually discarded by observation, stay on as uncertainties and thus risks to the observer in any further observations, and they can reassert themselves in the most inconvenient ways.

It must be made clear that there is a general failure in the risk-based approach to accept this situation. The observer cannot but make a distinction between what is 'the system to be observed', and what is by necessity left unobserved; the act of observation automatically includes both. The statement that the world is 'observable *because* it is unobservable' points to a revealing aspect, both of risk, and of the risk-based approach as it is commonly perceived. It points to the fact that there can be no such thing as a *non-risk-based approach*! The word 'approach' itself necessarily includes risk. It implies the generation of a distinction as a move out of an observer's inertia and the unavoidable difference between what is observed ('approached') and what is left unobserved ('unapproached'). The word

'approach' effectively demarcates an immediate need to cut down on the complexity in uncertainty, and as Luhmann remarks, 'complexity in this sense, means being forced to select; being forced to select means contingency; and contingency means risk' (Luhmann, 1995).

Thus uncertainty cannot easily be broken down into categories of risk, and even when this is attempted, as in the risk-based approach to AML, the uncertainty is merely transferred to these categories, but without losing any of its essence. All that happens is that risk gains a series of adjectives that incorporate their own distinctions and differences: financial risk, legal risk, structural risk, project risk, process risk, technical risk, and the like; all 'residual categories'. Meanwhile nothing has been said about the structuring of uncertainty into these subcategories of risk.

In attempting to control risk within these subcategories, the observer is in fact imposing a subsystemic description that interferes with the original larger system of risk, thereby changing it, but also introducing new risks and uncertainties. The very fact that all these newly imposed 'risk-subsystems' co-exist within the original system of risk changed by the categorization, immediately makes the subsystems themselves prone to the very same abstract phenomena that these categorizations in themselves are claimed to manipulate; namely those of uncertainty and risk. This is one form of the interference principle – all observation both disturbs and changes the thing being observed. Likewise, in categorizing risk, not only does the original risk remain, but also in the process new systemic risks are created amongst the categorized subsystems! Furthermore these new risks are unique to the observer/categorizer. One obvious example is that some stakeholders are concerned with the risk of launderers going unchecked, others with the risk of being jailed for failing to catch them.

What then is gained by such categorization? The process of separating risk into a multitude of categories has a goal. But is that goal achievable? The stakeholders (observers all) participating in such a process must think so, for why else would they categorize? They operate under the belief that risk can be better managed if broken down into these constituent subsystems. This belief, however, is just a characteristic of a reductionist mindset: a belief that studying the parts will lead to an understanding of the whole. Such a mindset is symptomatic of the lack of understanding of risk. As described above, risk per se is not a 'thing', and so does not have any constituent subsystems as such; all categorization is an act of choice imposed by the observer. Therefore, the process of breaking risk up into parts, even any original notion of risk, is artificially imposed by the observer, who must decide how that process is to be realized. Each individual, despite using the same categorical labels, will make different decisions.

ON THE REGENESIS OF RISK

When risk is broken down into subsystemic-risks (for example technical risk), it is easy to be deluded into focusing on such subsystemic-risks in isolation from one another, as residual categories, and quickly forget the many interactions amongst the many other aspects of risk that have been quietly abstracted away in the process of breaking up risk. Subsystemic-risks do not exist in isolation; they are structurally coupled to and interact with risks in other subsystems, an effect that any categorization has to accept, but which it cannot by default incorporate. This inescapable interaction at the level of subsystemic-risks creates more risk, which complicates matters further. Risk can therefore also be uncovered within the interaction of subsystemic risks, as *the very act of* interacting involves risks of its own. Such interactions go completely unnoticed, and if they were to be analysed, further categories would need to be created, and with such categories new interactions would unavoidably be introduced, and new risk, ad nauseum. This re-creates risk (again!) at the level of the entire system.

In this manner, subsystemic-risks interact in a multitude of complex ways that give rise to combinations of risks within and beyond their interactivity. That interaction therefore re-creates *risk out of risk*, thereby constituting an expanding self-referential system. The processes behind this regenesis of risk necessarily remain unobserved. Being considerably subtle, this regenesis cannot be pinned down for it is excluded the very moment risk is categorized. Meanwhile the original issue of confronting money laundering, the whole purpose of the exercise, all but disappears.

Such processes challenge each other, recoil from each other, permit or deny each other (Pinter, 2005), and much like in art, which cuts across causalities and creates something that can simultaneously be both true and false (ibid), risk contains 'the possibility of its own impossibility'. In art, and in the representation of art, such situations are familiar in surrealism that could perhaps hint towards this difficulty in representing risk, and in the possible permutations that such representations allow.

No matter how our interaction with the world is mediated, that representation of the world and/or any of its aspects (like risk) is a delusion. There is no optimum way of representing our interaction with the world. Even worse, just because some representations appear to be temporarily functional and relevant, we take a leap in believing that our current representation is able to represent reality accurately. The medium that is then used to facilitate this representation (be that a mathematical model or a series of logical considerations) is believed to be the one and only true

representation, and hence what mediates the interaction gives the delusion that we are actually confronted by the thing-in-itself.

In his painting, the Key to the Fields (*La Clef de champs*), artist René Magritte points out this way of thinking (the reader is encouraged here to search for this painting). He smashes the medium, the window on this occasion, into a thousand pieces. To highlight just how powerful and persistent a representational delusion is, even though the window is shattered, the shards of broken glass still carry the image of what originally lay behind each piece. A strikingly similar analogy can be attempted with uncertainty and risk: no matter what method is employed for breaking free from it, no matter what hammer is used to break the glass, uncertainty and risk persists.

THE CONCEPT OF RISK

According to Luhmann, the human approach to risk carries an important function: 'since Bacon, Locke, and Vico, confidence in the feasibility of generating circumstances has grown; and to a large extent it has been assumed that knowledge and feasibility correlate. This pretension corrects itself to a certain degree with the concept of risk, as it does in other ways with the newly invented probabilistic calculation. Both concepts appear to be able to guarantee that even if things do go wrong, one could have acted correctly' (Luhmann, 1993).

With the propagation of rationality and logic, the belief emerged that one can manipulate reality, and that within that reality one can create specific circumstances that are intertwined in cause and effect relationships, and subsequently manipulate them to ones benefit. The creation or generation of these circumstances has, as Luhmann remarks, generated an imbalance: a delusion in perception, a pretension that the world can be manipulated by knowledge that we create, regardless of the fact that this knowledge unavoidably implies both non-knowledge of something else, and a paradox at its foundational basis. The *raison d'être* of risk can therefore be seen as penetrating the core of this paradox; risk exists not because knowledge is possible but because it is simultaneously impossible; without risk, the demystification of the paradox would imply an ever greater paradox: that knowledge would be possible without any observation or representation whatsoever, for it would be only in that event that the whole could be understood. But certainly, such a world is far from the 'real world' human's experience.

Knowledge is being used to generate and construct specific circumstances in the world where we operate. Generating circumstances implies

a co-alignment of distinct possibilities that are linked together in cause/effect relationships. This ceaseless activity of attempting to manipulate the generation of circumstances must also imply a manipulation of risk, which is archetypical of all systems that attempt to control the outcomes of their interactions with the world.

Anti-money laundering (whether risk-based or otherwise) certainly belongs to this type of system, in that there is an attempt to control both the interactions and communications for the purpose of improving both the AML system itself, and also the outcomes of its interactions with other systems (the legal system) in order to reach successful prosecution of ML cases and consequently confiscate illegally acquired assets. Arguably, this obsession within the AML community for controlling processes and outcomes has thus far proved ineffective. As it has been amply demonstrated in the case of information systems influences on AML, even though technology is supposedly incorporated within financial institutions to control the processes for identifying suspicion, risk is induced at all sorts of different levels which cannot be easily identified (if at all).

Risk perpetually replicates itself, finessing all attempts at control, thereby generating anxiety and discomfort amongst all involved; consequently initiating yet more calls for risk to be controlled. As noted above, this situation is archetypical of all human activity systems obsessed with control. Anti-money laundering is no exception. In this sense, the risk-based approach to AML is equally problematic.

In undertaking AML, financial institutions and other stakeholders are being forced to make distinctions with the purpose of cutting down on the complexity that they face. Such distinctions necessarily imply that risk will be generated, even in the process of attempting to reduce complexity. Distinction implies change, and change introduces uncertainty. Consequently, risk is a necessary evil in any act of observation or decision-making.

THE 3RD AML DIRECTIVE AND ITS CONFUSION OF RISK

Much of the hyperbole surrounding risk and the risk-based approach in the AML domain came when Basel II expanded the prevalent notions of credit and market risk, and included operational risk. However, the qualitative nature of operational risk tended to confuse the more strictly quantifiable credit and market risk. Instances of this can be seen in the following extracts from Basel II.

The Committee on Banking Supervision wrote that it 'recognises that

the AMA (Advanced Measurement Approaches) soundness standard provides *significant flexibility* to banks in the development of an operational risk measurement and management system', while 'it is expected that supervisors provide flexibility in the practical application of such thresholds such that banks are not forced to develop extensive new information systems simply for the purpose of ensuring perfect compliance' (Basel, 2004) (emphasis added).

Two comments can be made immediately. First, the belief that the extensive deployment of information systems can 'ensure perfect compliance' is heavily problematic – as previous research findings have clearly demonstrated. Second, the fact that *significant flexibility* is being allowed to the financial institutions implies that the regulators cannot provide substantial guidance in dealing with the risk-based approach. The regulators have consistently refused to give advice on the particulars of previous AML compliance regimes, while simultaneously demanding compliance. That stance was ultimately indefensible, and the risk-based approach can be seen as a retreat from that unfair and dogmatic position. But this doesn't mean that the risk-based approach will actually work either, only that it is a political compromise, a way out of appearing as regulatory inert. As noted above, we now have the situation where the regulators are no more able to give substantial guidance on the risk-based approach than they were on previous approaches to AML compliance. Consequently the risk-based approach intended to reduce risk, can actually aggravate it.

Thus, the 3rd AML Directive of the EU, and its introduction of a focus on risk for the AML community, has complicated matters. Indeed, in certain respects the situation has become more confused. To illustrate the problem further, a deconstruction of various aspects of risk pertaining to AML within the Directive is attempted in order to highlight the confusion implicit in some key extracts that paradoxically are meant to clarify the situation.

The Directive refers to 'situations where a *higher risk* of money laundering may justify enhanced measures, and also situations where a *reduced risk* may justify less rigorous controls' (EU, 2005). The Directive then refers to: 'Member States that can focus their monitoring activities in particular on those natural and legal persons that are exposed to a *relatively high-risk* of money laundering or terrorist financing, in accordance with the principle of *risk-based supervision*'; 'member states that may decide to adopt stricter provisions, as reflected in Article 4 of the Directive, in order to properly address *the risk involved with large cash payments*'; as well as referring to the need for 'AML stakeholders . . . to ensure that the transactions being conducted are consistent with the institution's or person's

knowledge of the customer, the business and the *risk profile*' (italics added for emphasis).

The document further refers to the need for 'institutions and persons . . . to determine the extent of such measures on a *risk-sensitive basis* depending on the type of customer, business relationship, product or transaction' (ibid). The Directive goes on to talk about the handling of '*low-risk* of money laundering or terrorist financing which must meet the *technical criteria* established', and the need to have 'adequate and appropriate policies and procedures of customer due diligence, reporting, record keeping, internal control, *risk assessment*, *risk management*, compliance management and communication in order to forestall and prevent operations related to money laundering or terrorist financing'.

From the indicative extracts presented above, the following observations on how risk is represented within the Directive can be made:

1. First, the text of the Directive refers to the *hazardous aspect of risk.* However, as we have seen, risk can also present itself as opportunity. In 'taking a risk', hazard and opportunity are opposite sides of the same 'risk' coin, whereas 'being at risk' emphasizes hazard alone. But all action involves risk. There is no such thing as a risk-free approach. The term 'risk-based' is a tautology, it is a use of words that doesn't actually admit to anything other than the fact that risk exists. The drive for a 'risk-based approach' is a tacit recognition that risks have to be taken in search of commercial gain. In AML, however, a risk-based approach regarding the targeting of money laundering refers to the occasion whereby the distinction of suspicious/non-suspicious potentially – and mistakenly – collapses into the condensed form of non-suspicion alone. This raises the possibilities both of leaving a set of truly suspicious cases unreported to the FIU, and of reporting innocent individuals as suspicious. Such possibilities need to be further accepted by the regulators, who by their own statements are supposed (at least in principle) to operate within the realm of risk-based supervision, and hence refrain from the imposition of financial fines if the institution has in place sound processes for the management of risk; whatever 'sound' may mean.
2. A further distinction for risk is used within the Directive, namely between *high-risk* and *low-risk.* In proposing levels of risk, they are implying that risk can be quantified, but without explicitly stating how. With no yardstick, such quantification can only come from qualitative mechanisms that will somehow distinguish between high and low risk. Any such assignment of probabilities or numerical representations to risk is problematic, as it posits an epistemological anomaly:

that risk can be represented by something that lies somewhere in the 'grey area' between quantitative and qualitative analysis.

3. Furthermore, within the scope of the Directive, there are considerable implications for what is referred to as *risk-based supervision*. Regulators will need to be more flexible themselves in their interpretation of compliance with Anti-Money Laundering guidelines. By necessity, risk-based supervision implies risk-based compliance, which in turn introduces the potential for (the risk of) considerable friction between AML stakeholders and regulators. The problems inherent in such vague notions of compliance, therefore become ever more crucial as compliance cannot be easily quantified (for example a bank cannot be 84 per cent compliant). The risk-based approach makes compliance even more complicated, because the risk of leaving a potential money laundering case unreported still has to be addressed, but now the regulators must recognize that occasional failures are unavoidable. In a letter to Ian Mullen (Chairman of the Joint Money Laundering Steering Group), Philip Robinson (Financial Crime Sector Leader of the FSA) showed awareness of this risk when he stated that 'we recognize that some firms have concerns that if they follow a risk-based approach we might challenge their actions on the basis of hindsight, and sanction them for any misjudgement. But if a firm demonstrates that it has put in place an effective system of controls that identifies and mitigates appropriately the risks for ML, enforcement action is very unlikely'. The words 'effective' and 'unlikely' themselves can only be justified in hindsight, and so actually introduce yet more uncertainty, and hence risk, because they imply that enforcement action may occur at some later stage for yet unspecified reasons. Thus Robinson's statement, far from comforting financial institutions, may well increase their compliance fear and uncertainty. Within the vast gulag of internal processes and controls deployed by a financial institution, how will failure to comply be attributed? To a particular set of processes, or to individuals? And by what standards will such judgments occur? How will risk-based supervision be put into practice when the internal document that is the basis of checks by the Financial Services Authority is labyrinthine? Even the Chairman of the FSA accepts this to be a problem (and thus a risk): 'The policy question is the balance between the two, and in particular the extent we can rebalance between the present very large (8500 pages and growing) rule book on the one hand and principles on the other. . .This rebalancing will not be easy' (McCarthy, 2006).
4. The Directive does actually refer to the creation of *risk-defined parameters*, and the process of parameterization for the risk-based approach

becomes a little more concrete and explicit. Risk is represented by various parameters related to money laundering, such as large cash payments. Such parameters can be viewed as proxies for modelling money laundering behaviour, however, they are likely to lead to knee-jerk acceptance among compliance officers that all large cash payments are suspicious, and thus an increase in the reporting of false positives. In other words there is a risk that the distinction between suspicious/non-suspicious will become a bureaucratic decision and that the code for the AML system will be reduced to ticking boxes once again.

5. There is also mention of *risk-defined profiles* that can be used for targeting ML. A risk-profile is typically an agglomeration of different risk-defined parameters meant to reflect the particular vulnerabilities of a financial institution, taking into consideration its clientele. These profiles are usually enriched with additional intelligence so that complexity is reduced, and the number of possible suspicious transactions minimized so that it matches the testing capacity of money laundering analysis teams. However, it has the same failings as above.
6. Following mention of risk-defined parameters and risk-defined profiles, the 3rd Directive then turns to the concept of *risk-sensitivity.* However, it quickly becomes evident that the concept of risk-sensitivity is even more elusive than risk itself! How does the concept of risk-sensitivity stand up, when in effect it is asking 'how risky risk is'? How much of this terminology has any scientific basis, and how much is it wishful thinking? The elaborate schemes proposed are not sufficiently understood by those who created them, let alone by those responsible for putting them into use. How can they possibly be meaningfully put into practice? A question that is valid about the whole 3rd Directive, and not just its musings on risk sensitivity. In this chapter, an application of the risk-based approach will be presented through a data-mining application. This application will be presented not as a solution but as a way to think in systems theory terms about this particular problem.
7. The misrepresentation of risk and consequent vague specifications are inevitable whenever risk is attributed with having *technical aspects.* This implies that there is an emphasis within the Directive on adopting technology and the risks that this adoption brings. From a systemic point of view, the systemic aspect of technology, and the risks that it implies, transcend the merely technical aspects as they mingle with human activity systems to create a complex fabric of information systems. The integration of technology into AML procedures has been extremely problematic thus far, mostly because the systemic

emergent properties of information systems have been rarely considered. Nothing in this regard has changed with the 3rd Directive.

8. Finally, nearly all of the above aspects regarding risk need to be assessed and managed, something the 3rd Directive itself emphasizes. This then becomes one of the most challenging aspects of *risk-assessment* and *risk-management* in that mechanisms for improving the already existing methods for handling risk need to be investigated.
9. These observations and comments on the risk-based elements of the 3rd AML Directive by no means exhaust all the aspects of risk. However, by providing just a few examples, some intrinsic (and very real) difficulties in handling the relationship between risk and AML are exposed. The risk-based approach must itself be confronted for it involves some crucial and pragmatic choices, none of which can be made without considerable reflections on how risk is represented within the context of AML.

RISK REPRESENTATION

Before the different yet distinct stages for representing risk are described, it would be useful to sum up the aspects of risk introduced thus far. At this point it is helpful to distinguish between: 1) the processes of risk-representation, and 2) the management of the processes for risk-representation. Such a distinction could be viewed as constituting two distinct domains. The domain that refers to the processes of risk-representation would entail: a1) parameterization, a2) quantification, a3) profiling, a4) sensitivity, while the domain that would refer to the management of these processes would entail: b1) assessing, b2) managing, and b3) supervising these processes.

But even more important than the representation and the handling of risk, is the communication of risk between stakeholders which factors into each stakeholders' interpretation of the code of the AML system. Financial institutions must insist on the benefit of both cooperating with other stakeholders for identifying areas of common interest, and elaborating techniques for representing and handling risk. At the same time, financial institutions must communicate the manner in which they represent and handle risk to the FIUs and the regulators. On their own account, FIUs and regulators need to organize their own internal risks, and communicate them to those stakeholders that are responsible for the production of STRs, and those that are monitored for compliance against AML regulations. This ongoing feedback loop of communication of risk representation and handling is perhaps the only way to conceptualize a

risk-based approach within a national AML system. Systemically, it is supported by granting primacy to the concept of *communication* and the important function that it serves for the exchange of information between different systems within society. Otherwise stakeholders will operate in isolation, their internal processes for handling risk will become hidden, and any hope of realizing the potential of the AML system will be lost.

To sum up, the following aspects of risk can be delineated:

1. Risk as an independent entity exists regardless of our efforts to manipulate/reduce it, and all the while it persists via uncertainty in a regenesis.
2. The representation of risk takes place through a series of different methods like parameterization, quantification, profiling and risk sensitivity.
3. The communication of risk-representation is essential, so that respective parties can gain a consensus on what methods are being used. This does nothing to reduce the risk of communication itself, since that too is based upon a further distinction of what is communicable/non-communicable.
4. Dynamic feedback should inform the representation of risk, and hence the methods for parameterization. This is crucial for a system like AML that is structurally coupled with money laundering techniques, which continuously change, re-group and exploit deficiencies within AML.

A cynical critic of the risk-based approach would probably be able to spot the fact that the Commission's attitude to the risk-based approach is actually risk-averse! As it stood originally, it was particularly difficult to force well-structured ways with which the AML system could 'control' the money laundering problem. The Commission eventually decided to mitigate the risk of preserving guidelines for control, and recommended the introduction of the risk-based approach. Then, however, a very interesting irony came to the surface: risk is so elusive that it can be introduced by attempts being made to mitigate it.

THE CONSTRUCTION OF RISK-DECONSTRUCTION

Some important changes come with the introduction of the risk-based approach. First of all, the shift within the risk-based approach focuses on the construction of models, instead of the examination of individual cases. The construction of the models is informed by the various risk elements

(parameterization, and so on) that we described previously. While it must be recognized that there is a broad shift in and consensus for describing the risk-based approach to AML by moving from the specific to the general and by improving processes that surpass the equal consideration and scrutiny of all-cases, a further clarification will be attempted that points towards a foundational mistake when it comes to representing risk.

We have already seen that within the risk-based approach there appears to be considerable complexity in representing risk, and that such a complexity ultimately needs to be simplified. Such simplification is not a compromise, but an unavoidable necessity. The question then becomes considerably subtler: how does one cut down on the complexity of representing risk within the risk-based approach for AML?

Typical methods to tackle the problem of multiple risk-representations and the complexity behind them, involve the construction of matrix-based risk attributes. In other words, a matrix is created where different risk-attributes are neatly broken down and categorized while being given a numerical representation. An example of this would be to separate between product specific risks and firm specific risks, but by far the most popular one is the likelihood/impact model that deals with the calculation of risk once the likelihood of an event (that is, suspicion) and its impact are probabilistically calculated. An event, for example a customer in a potentially 'high-risk' zone of ML suspicion, can be assessed according to its likelihood (the possibility of the event occurring) and its impact (cost of internal investigation, organizational, compliance-costs, and so on). Two initial problems then become visible. How can one provide such an assessment, and how can a number be assigned for either the likelihood of an event or its impact? Even worse, if combinations of events are considered (networks of ML instances) then a probability would be required to account for the interaction between different yet complementary events.

Many analysts, and indeed the FATF itself, recommend a delineation into 'high- and low-risk' products or services. For instance, products and services such as private banking, correspondent banking, wire transfers, e-banking and use of credit cards are typical examples of *perceived high-risk* for ML. These can be then categorized in a potential product/risk matrix in order to examine the volume of activity, to monitor the potential risks that are faced within each institution, and to demonstrate a prudent methodological structure for compliance purposes. Similarly, high-risk customers are also considered for which typical risk-scoring systems can be created; money transmitters, cheque cashiers, security brokers and dealers, property dealers, professional and consulting firms and so on. The list goes on and on. According to the risk-based approach, exporters, importers, and all cash intensive businesses (retail, restaurants, second

hand car dealerships, offshore corporations, banks in secrecy havens, as well as non-profit organizations like charities) are increasingly being manipulated by launderers. Thus this group of high-risk customers should head the list of those being reported.

But the fact that we can designate such categories does not necessarily mean that such categories can automatically incorporate the totality of a single category (say high-risk customers). This is the foundational mistake of the risk-based approach. It needs to be made clear: there is nothing intrinsic in any of these categories that can force them into being designated as high-risk for money laundering. In fact, it quickly becomes evident that the regenesis of risk is passed onto its designated subsystemic categories, while simultaneously none of these categories can be intrinsically classified as being of high-risk. Any category can, at the same time, be both part of the high-risk and low-risk assessment process. For example, let us take a cash intensive business like a retail store. Once one defines that to be a category then it is inevitable that varieties within the same category (namely different retail stores), risk-subsystems in themselves, will be part of both high- and low-risk assessment processes regarding money laundering. Any category itself is therefore a risk-based hybrid! When the category opens itself up for classification as qualitatively either 'high' or 'low' risk (before being assigned a numerical probability) it cannot resist being simultaneously part of both 'high' and 'low' risk areas. This simultaneity owes its nature to the malleable nature of risk itself and the considerable difficulty that is placed in its abstract nature.

Given that any category can be portrayed as a risk-based hybrid within anti-money laundering, the current modus operandi of classification of ML-risks is simplistic. It is an anachronism based on the fundamental misconception that risk becomes diffused once broken down into its subsystems (risk-categories), a misconception that cannot withstand proper analytical scrutiny and one that does not recognize the gravity of the problem of the reflexivity and regenesis of risk. At the same time little guidance or consideration is given (both in academic research and industry) to how this problem can be dealt with. Little emphasis is placed on methodological aspects that could be utilized to inform the construction and exchange of risk-based feedback processes.

The problem of the regenesis of risk has no solution. Of course, how can there be a solution when the only systemic function of solutions themselves is to 'multiply, proliferate, disperse, circulate, diversify, diffuse the original problem' (Rossbach, 1993)? The very best that one can do is to provide some systemic considerations on how the de-construction of risk could be attempted in light of feedback mechanisms between financial institutions or other AML stakeholders with FIUs, and go on further

to provide some thoughts on how AML stakeholders can demonstrate a prudent deconstruction of risk.

A DATA-MINING APPLICATION FOR THE RISK-BASED APPROACH

What is presented in this section is a data-mining application that essentially follows the spirit of the risk-based approach, despite all of the shortcomings that have been extensively analysed in the previous sections. This approach was applied to a financial institution in an EU-country and was originally developed by the author in the year 2004. This approach was subsequently enriched substantially by a series of techniques the financial institution developed itself so that it would include data from additional sources besides raw transaction data. As it will become evident, the entire application was the result of a systems-theoretical approach. While it was reported to the author that substantial improvements were experienced by the financial institution (in increasing the true positive rate of STRs), this approach is not presented to be a solution in itself. Systemically, a number of variations on this approach can be attempted.

For the purposes of this last section, the author will somewhat change the style of writing to a more informal one and attempt to describe the story of how part of the theoretical treatise exposed in this book has come to be applied for a first time in a financial institution in an EU-country and has influenced the author's viewpoint regarding what is now known as the *risk-based approach*.

The technique, about which this section is written, was conceived of almost accidentally while thinking in systems theoretical terms about a pragmatic problem that required exploration. I shall describe here the events as they unfolded, briefly, yet accurately (as far as my memory allows), and always in the first person singular, so that the events are told as vividly as possible.

In the year 2004 I was working at the London School of Economics as a research analyst for a European Commission project on AML. From my personal research into the field of anti-money laundering I was already aware that when it came to technology and AML, the results were really poor. At the time, the industry average rate of True Positives was about 4 per cent (as suggested by the FSA – the reality was that much lower TPRs were observed), and thus for every one hundred suspicious transaction reports flagged by technology, only four came out being truly suspicious after careful manual examination by ML-analysts. By anyone's standards, and despite the difficulty and complexity of the problem domain, I thought

that was rather poor. It still is, but when it comes to technology determining suspicion, it has never been easy territory. The automated modelling of money laundering faces a considerable amount of ambiguity which arises from four factors (Canhoto and Backhouse, 2007). ML does not correspond to any one particular behaviour, it involves a variety of actors, the form that it takes is continuously evolving and its modelling is prone to a number of information elements held by different institutions that 'do not exchange information easily, owing to legal, strategic, and operational reasons' (ibid).

In dealing with the issue of attempting to model ML, our team requested a large financial transaction dataset (of raw transaction data) that would be extracted from the financial institution. This dataset would be used for the simulation of models for ML, but no one could actually articulate what those models would 'look like', how effective they would be, how they would be tested and so on. In fact, as far as I could see at the time, no consensus could even be made about what might even constitute a 'model'.

After a series of negotiations with the head of the money laundering analysis team, we began the necessary work for extracting the transaction dataset. This lasted for about three months as we needed to test the format of the database, ensure that there was data integrity, and mostly, that personal details like names and addresses were removed. Anonymized modelling of ML, however, was somewhat of a novelty at the level of raw transactions so it had to be dealt differently. Banks usually don't share their raw transaction datasets. There was a need therefore to associate customers with substitute codes so that we could know what transactions corresponded to the same people. Thus, Dionysios Demetis for instance became SEC01363845, an *unidentifiable alphanumerical combination* for which however different transactions in different points in time could be linked. The relationship between the unidentifiable alphanumerical combination and the real identity of the customer was only accessible to the financial institution itself.

The anonymization process was one story. The other one was the extraction of the raw financial transactions and their manipulation for the purpose of spotting suspicious behaviour linked to ML. We were discussing the time frame for these transactions so we decided to have at least 3-months of data. The extraction process took several weeks because of security reasons and then the data were sent to me at the LSE. A colleague still recalls the horror engrained in my face when I was faced with about 15 DVDs containing approximately 250 million financial transactions. Fortunately, unlike the HM Revenue & Customs loss of data on 25 million people,[2] our transactions were not lost but had been anonymized in case of such an event.

So far so good. I will omit a lot of technical details of how these transactions even came to reside in a single database for manipulation, and cut straight to the point. What does one do with 250 million raw financial transactions when looking for suspicious ones?

My opinion was (and remains) that there are two distinct possibilities if you want to analyse financial transactions for ML:

1. You have a model for ML. That model describes ML as best as possible through a series of parameters. You then apply that model to the financial transactions and receive a set of transaction data that are considered to be suspicious. The staff members of the financial institution subsequently examine that set manually, and it is determined (case by case) what occurrences within the set are really worthy of submission to the FIU as potential ML-cases.
2. You attempt to deconstruct, from financial transactions, *specific transacting patterns* that could potentially relate to suspicion. This deconstruction does not use any model that attempts to separate suspicious transactions from non-suspicious ones. Rather, it occurs as a bottom-to-top process. Data can potentially be data-mined and subsequently patterns of transacting behaviour may emerge from this more granular examination of a dataset.

In the first circumstance I thought results were really poor anyway. A problem of such complexity cannot be modelled easily. Launderers exhibit considerable variation and if you attempt to model their behaviour as a top-to-bottom process then you would need to construct categories for each of the identifiable behaviours (or sets of behaviours). This implies that the real behaviour-deviations from the projected abstract categories will create a series of problems. Financial institutions in the country where this financial institution was based (another country to where Drosia bank was based), used about 6–7 parameters for modelling ML in an automated fashion. So much for those overly expensive software packages that came with more than a hundred predetermined queries to simulate ML. The actual parameters being used by financial institutions were quite simple, and mostly had evolved around age, location, time of association with the financial institution, and so on.

But let us go back to the problem. What does one do with 250 million financial transactions? According to the two methods presented above, the first one would be impossible for the scope of a research project. It would mean that we would have to take precious time out of the schedule of already busy staff members that deal with ML-cases in order to test all sorts of different models and see if what they come up with is confirmed

as truly suspicious after proper scrutiny, KYC and the like. This path was never taken. I had the feeling it wouldn't work anyway after a discussion I had with the head of the statistics team who said to me that 'you may have a profiling query that tries to capture ML behaviour and it may be idle for 6 months or more. Then one day, it may flag out something that may turn out being suspicious; with these things you never quite know. It's not as if there is a pattern or anything.'

This rather disheartening assertion is quite important. Indeed, the element of time is absolutely crucial in every pattern-seeking mechanism such as spotting suspicious transactions. You may have a query that is supposedly capturing a sequence of transactions that simulate ML-behaviour but it may not prove to be fruitful until an actual laundering case is investigated. Meanwhile, the query remains 'idle'. But is it really? Can it ever remain idle? The answer is no. Until useful cases are uncovered, any query generates volumes of false positives and therefore time is an essential element that forbids ample experimentations on ML-behavioural patterns.

Thus, it is worth investigating the option of a bottom-to-top approach; that is, to deconstruct, from financial transactions, specific patterns, or even better, specific characteristics that could potentially be related to suspicion. I started looking at the second possibility more closely and differentiated the question slightly to accommodate the new possibility. How does one manipulate 250 million transactions without imposing a model for cutting down on the unnecessary complexity?

First of all, the problem was not only one of complexity, but also of volume. Manipulation of that large a number of transactions is uncommon (at least for daily practice) for the second technique of bottom-to-top manipulation. I thought that similarities would have to be drawn to other disciplines that deal with uncommonly large datasets, and I would have to investigate how such disciplines make systematic inferences from within the data. As a former physicist, I immediately thought of the field of astrophysics, so I started looking into the manipulation of large numerical datasets there. I always thought that the key to such a complexity remains in the visualization of the data along with the possibility for interaction of that visualization, processing and methods of cutting down on the complexity.

And so after some time I managed to project the 250 million financial transactions on a 3-dimensional malleable plane that could be manipulated, rotated, parameterized, filtered and so on. I must say, it looked beautiful (not a little irony is included in this assertion). But it wasn't of any help whatsoever. It looked like a constellation somewhere in the universe, and the telescope was supposed to find 'suspicious transactions'.

I played around with it, but abandoned it almost immediately. I came to realize that complexity is a fundamental systemic property of any system, but most important of all that it is a *transcendental property*. This idea of complexity as a transcendental property cannot be stressed enough. It implies that transactional complexity mutates into numerical complexity, numerical complexity into profiling and algorithmic complexity and the latter mutates into visual complexity. Systemic complexity may change form or shape but always remains present.

I went back to the last settled question: 'How does one manipulate 250 million transactions without imposing a model for cutting down on the unnecessary complexity?' and started pondering the issue of the constitution of a model. Something had to be applied for inferences to be made and complexity to be reduced. But what would that something be? What model should attempt the reduction in complexity?

This systemic re-arrangement in the form of the above question made all the difference as the model came to be something completely different from an association of parameters describing what a money launderer should look like. Based on the theoretical grounds of systems theory I had followed the premise that systems are most of all self-referential. They have mechanisms for referring to themselves and to their constitutive elements, they create internal system/environment differences, and hence they create internal differentiations. Systemically, if any perceived improvement (for the system itself) is to take place it therefore has to be based on two basic characteristics. It has to generate a distinction or difference and it has to utilize that difference by means of a second-order observation (it has to observe how it is observing). With that systemic principle, I sought to identify the distinction that could be thus utilized, and further to consider the issue of second order observation. It turned out that even though these two were intertwined, the latter step was much more interesting in its exposure (and relation) to ML-modelling. The STRs submitted by staff members were distinguished into two categories:

1. Those that were found to be positively suspicious after manual analysis by the AML-team and were consequently submitted to the FIU), and
2. Those that were not found to be suspicious after manual analysis by the AML-team.

One side to the distinction had to be chosen for application, but it is worth noting that – for the description that follows – complementary (yet different) results would be retrieved had the second option been chosen instead, and of course, different distinctions can be utilized for the purpose

of uncovering elements of suspicious behaviour within raw transaction data.

However, the purpose on this occasion was not to spot suspicious transactions. It was to 'reverse-engineer' the process of STR-production and extract a set of characteristics that could be used as a mechanism for modelling the behaviour of money launderers. As those characteristics would have to be used within the scope of automated technology (which was performing rather poorly), the issue of effectiveness was put into question within the distinction between manual versus automated True Positive Rates. For instance, whereas staff members performed very well, and typically around 50–60 per cent of the potential STRs that they forwarded internally to the MLRO would turn out as truly suspicious after manual examination, technology did poorly (at around 1–2 per cent). All the difficulties created by the poor performance of any technology-based solutions could therefore be repositioned in the form of a feedback loop between the manual generation of STRs and the automated rules for establishing suspicion. In other words, the point was to establish a mechanism that would take advantage of the relative success that staff members have had in reporting and feed it back to technology-based suspicious generations.

For this purpose, and to see what was the qualitative and quantitative information that could be extracted from all these millions of transactions, I changed the concept of a model for ML by admitting to the following: a model is not only what simulates ML behaviour and breaks it down to all sorts of different attributes that describe who potentially is a money-launderer. *A model can be anything that reduces the initial complexity* of transaction sets in order to infer further characteristics that may in their own turn recursively redefine how we view, simulate and model ML. In this regard, any data from fraud, marketing, demographic, media, statistics, criminal, police, and other sources could have been used.

Instead of creating a top-to-bottom process that specified what money laundering characteristics would be, another model was created (of a somewhat different type). I asked the head of the ML-analysis team of that financial institution to give me all the account numbers of customers that had already been reported to the FIU (of course after they have been scrutinized by members of staff as being truly suspicious). These were in the reference form discussed previously (for example SEC39476423), whereas the original account numbers remained with the financial institution. The question that can be put here is: 'Can a long list of account numbers constitute a model for ML?'

The answer is in the affirmative provided that the model is used to differentiate the transaction sets and reduce the underlying complexity. Its specific function is to be applied to the totality of the available transaction

set, and to act as a filter that isolates from the totality of the transactions that take place in the financial institution only those raw transactions that correspond to the account numbers that are specified in the model. These account numbers are those specified before, that is, those that correspond to customers that have been already flagged as suspicious for ML and forwarded to the FIU.

The entire process is described in detail in the list below:

1. First, we may differentiate between staff reports that are further considered to be suspicious and those that are not. This is only possible after ML-analysis teams examine each STR one-by-one and determine whether further reporting to the respective FIU is necessary.
2. The reports that staff members send from the branch-network of a financial institution and that are considered to be suspicious after careful manual-examination from a ML-analysis team, are typically logged onto a Case Management System regardless of their forwarding to the FIU or not. Various data fields are kept within the Case Management System for which a typical field would be the account number.
3. Extraction of the following subset of the Case Management System therefore becomes possible: '*all the account numbers of those customers that have been considered to be suspicious after manual analysis from staff members of ML-analysis teams*'.
4. A query can then be performed to isolate from the raw transaction data of a certain period (say the past three months), a subset of raw transaction data that corresponds to *all the transactions that have taken place by such customers.* The content of the query itself is quite simple, thereby constituting of an x-line query (say in SQL) where x equals the total number of customers identified in step 3), and where each line corresponds to an account number.
5. The output of this query on the totality of the raw banking transaction data becomes *another raw transaction dataset*, but one referring only to customers that have already been identified as suspicious following the initial manual examination. This new raw transaction dataset effectively holds information on the transacting patterns followed by potential money launderers. Further discovery of such patterns and their isolation can be done through data-mining software.
6. The discovery of trends and the customization of this methodology remain at the core of the selection of particular parameters and characteristics for further modelling. Thus, if say a financial institution is holding y-number of data-fields in their transaction databases, and only 10 per cent of those data-fields appear to be present in ML-

behaviour (for their own clientele and customer-base), then it makes sense that efforts around the selection of parameters and so on would have to be appropriately customized around that 10 per cent.

With this methodological structure, the output of the process remains distinctly different from what could be achieved with a normal statistical analysis. Day-to-day transactions corresponding to people already considered suspicious and reported to the FIU are isolated from the greater total transactional sets. In this manner, complexity is reduced while important information can be extracted from this endeavour that reveals money laundering behaviour that could be further used for modelling purposes. So what? What can be gained by following such an approach, and why can it be described as a second order observation in theoretical terms? What does it have to do with the risk-based approach?

The connection and the reply to the above questions can be made simpler if we are to follow an example that would clarify it. The reduction of complexity that was achieved by this technique was considerable. From the initial 250 million transactions, a few hundred thousand were left that corresponded to those account numbers that constituted the filtering model. Nothing however could compare that reduction (which still produced a considerably large amount of transactions but more manageable) with the further surprising reduction in complexity that was uncovered by means of data mining and by considering different categories.

For instance, from a total of more than 100 transaction categories that were recorded at any single time in the transacting databases of the financial institution, following data-mining and manipulation of the raw transaction data that corresponded to previously suspicious customers, only 14 transaction categories were identified as relevant to those that have been already reported for suspicion (these corresponded to more than 10 years of cases of ML-suspicion logged onto the Case Management System). These are portrayed in Figure 6.1.

Even further, what becomes evident within those transacting categories shown in Figure 6.1 is that from within the subset of transacting categories that appear to be more relevant for ML cases, there are particular transacting categories that occupy a larger percentage in the overall distribution.

This exposes a connection to the risk-based approach as the likelihood of suspicion for a ML activity may come to rest upon a fabric of interdependent characteristics that are isolated from raw transaction data. This implies that there is a higher propensity to consider someone as a suspicious customer when specific characteristics are considered. If say a customer is transacting in one of the major categories that take up a large part of the distribution in Figure 6.1, then a probability may be assigned

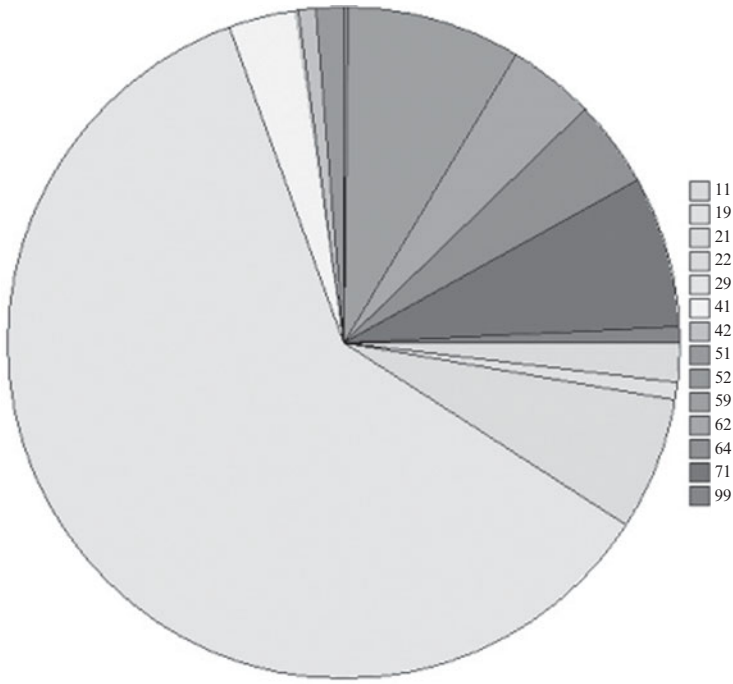

Figure 6.1 Distribution of transaction categories

to such a customer; a probability that may quantify the likelihood of someone committing ML. The estimation however of such a probability does not have to be associated to transacting categories alone. A series of other characteristics can be used for the same purpose (demographic, socio-economic data and so on).

In presenting some of this work in a number of seminars for government agencies, central banks, and financial institutions around Europe, I have come to realize that there appears to be a consistent point of confusion that most people in the audience will relate to. They ask whether it is possible to use this process when in fact it will only give you things you relate to cases you already know (about previous money-laundering cases). Quite often it will be confused with some automated 'supervised training' approach.

Another conceptual term needs to be distinguished here in terms of modelling money laundering; that of *behavioural modelling*. Whereas a model is a collection of attributes regarding suspicious behaviour, a behavioural model attempts to synthesize information from a series of

social, economic, demographic, cultural, political and other domains that can be used to model the behaviour of a launderer. Behavioural modelling in conjunction with the process described previously, not only gives a dynamic nature in the process of modelling ML-behaviour, but also places the modelling of suspicious cases on a risk-based attribution of characteristics.

I have always felt that if any improvement is to be made in this aspect of modelling money laundering behaviour then there would be a need to consider modelling beyond the classical realm of *typologies* that are published so widely (like those coming from the FATF). This implies customization at the level of the financial institution and presupposes that every financial institution has a different clientele base, something that is dependent on a variety of factors like location, network, and others. But as every financial institution has its own clientele base, it also has its own suspicious customers' base. Certainly, a bank customer in England is similar to a bank customer in Italy, or Greece, but then again there are considerable differences in their socio-economic, cultural and demographic characteristics that may 'reflect' somehow on their transacting behaviour. The same is the case for customers that are considered to be suspicious for ML. Decomposition therefore of those characteristics that are more relevant for the suspicious customers' base of a particular financial institution makes the risk-based approach even more relevant. As a typology is an abstract entity that attempts to encapsulate interdependent characteristics that may (or may not) describe what money laundering is, attributes that are extracted behaviourally in a bottom-to-top fashion and touch upon the specificity of a single financial institution have a better chance of being integrated and incorporated within a risk-based approach.

Of course, the example that was discussed previously regarding the risk-based attribution of transacting categories is the simplest example possible. The plot thickens when one considers combinations of different characteristics that may be used for the purpose of modelling and where one can combine in such a risk-based manner more than one attributes (say transacting typologies, location and so on). Subsequent profiling of suspicious customers then acquires a different character; one that is informed not only by already known typologies but also of behavioural characteristics of the pre-established suspicious customer base of a specific financial institution.

The difference therefore relies specifically on a second order observation of the system itself. What *essentially and informationally constitutes a financial institution* is carried – as information – through the individual financial transactions that are recorded in the institution's databases. If

we consider financial institutions as systems then transaction data is the platform through which they interact with their environment. The information extracted from such databases is also the systemic mechanism for other system/environment interactions (for example with the government) or indeed the trigger for decision-making processes (such as investments). In other words, a financial institution viewed as a system, functions by either allowing interaction with its environment and renders that interaction at its databases that hold transaction data, or by creating other financial instruments that once again, structure the interaction with their environment. The recent financial crisis that led to such a degree of destabilization is a result of a number of systemic consequences of complexity that where based on processes of positive feedback on various system/environment interactions. The crisis constituted, in effect, ample evidence that we have no idea how to deal with risk, other than that which we structure in particular rigid ways and then delude ourselves with our capacity to manage it.

Anyway, to return to the matter at hand, from a systems point of view, resolution or even an attempt of manipulating previously known information of other types (such as previous STRs) must be brought to the level of financial transactions and recursively be affected by them. How institutions observe is therefore equivalent to how institutions set themselves up to receive information, which is both organizationally and technologically structured. For financial institutions, such information becomes structured in the form of financial transactions and it is those transactions that informationally constitute the way in which the institution observes. For a second order observation to take place, another observer must be introduced that will guide another observation. Such a subsequent observation will – via a secondary frame – utilize raw transaction data and reconstruct the information they encapsulate on the basis of a secondary distinction (imposed by the frame).

What is further used to guide the observation is what we could call a *frame* for that observation. In this particular example, that *frame* has been the set of account numbers of customers that have been already identified as suspicious after careful manual analysis and inclusion in an original STR. The set however could have been considerably different. For instance, fraud data could have been utilized, or marketing data, leading to demographic characteristics that could enhance modelling aspects of ML. Combinatory possibilities become endless as elements can be reproduced and recombined.

In dealing with this problem, the methodology described above was applied to a financial institution in an EU-country and was further enhanced by the institution itself by the use of profiling data for simulating

money laundering behaviour on the basis of socio-demographic data (those were bought off a private company and the marketing department of the financial institution helped in their analysis). The externally bought data was utilized to enhance particular profiles, thereby estimating the propensity of someone being involved in money laundering activities.

This endeavour within the scope of this methodology (based on the self-referential re-informing of suspicion) created considerable dynamics in the adaptation of technology to the simulation of ML-behaviour. This resulted into a gradual increase in the True Positive Rate of the financial institution. In the very start of the implementation of automated technologies, the True Positive Rate was less than 1 per cent (how many reports flagged by technology are considered to be suspicious after further examination). This was improved gradually up to 17 per cent in the year 2006 and has remained around 15 per cent since that (according to data discussed in January 2010). For the STRs reported by staff members, the TPR is much higher at around 65 per cent.

This increase might suggest that the true positive rate of technology can be attributed to its association with an increase in the effectiveness of staff-member reporting. Even though the increase clearly suggests that there has been a dramatic improvement in the success of staff members reporting suspicion, it is unclear whether this success can be correlated with the improvement of the automated monitoring of technology (as further data would be required for this correlation). Considering however that the feedback loop between manual/automated is informationally exploited within its duality, the relationship appears to be close (even though an increase in the true positive rate of manual reporting can be attributable to increased vigilance, continuous training and so on).

With the improvement observed in the example outlined in this section, it is useful to consider the function of the risk-based approach within this description. It is of course clear that the very introduction of the risk-based approach implies some sort of prioritization. The purpose of the risk-based approach in itself has been to reduce the complexity that is generated when financial institutions and other stakeholders within the broader AML system report excessively to the Financial Intelligence Units, thereby creating a considerable increase in white noise. However, for the effective reduction of complexity it is useful to ponder the question of how risk can be represented and subsequently attributed to the entire process of simulating ML.

What has been outlined in this section constitutes both a method for a representation of risk at the level of interaction between different financial transactions, and a recursive mechanism that exploits these financial transactions in order to deconstruct the suspicious customer base. This in

itself is something considerably different to an analysis from within the cases of STRs themselves.

With that in mind, I think it would still be useful to stress that risk constitutes a highly elusive entity, and that whatever representation, manipulation, and application is attempted will generate a further risk. This creates another system, which is also self-referential in nature as risk is generated out of risk when categories are considered for any modelling process.

It is therefore very difficult to predict any long-term effects of the introduction of the risk-based approach on the broader AML system. For the time being it would appear that financial institutions are somewhat nervous of the regulators' interpretation of the risk-based approach. Risk-based supervision and tolerance of money laundering cases if proper 'systems' and organizational structures are in place at financial institutions is not much consolation due to the very nature of risk (thereby extending suspicion). From a regulatory point of view, a standard approach in dealing with the subject matter of the risk-based approach is extremely difficult (if not impossible) to attain and this affects a variety of AML-related aspects within a financial institution (and ultimately compliance itself). Overall, the shift towards a risk-based approach does constitute an improvement as it structurally couples with the elusive nature of suspicion. Risk and suspicion are therefore bound together and it is right that more restrictive practices have been abandoned (or claimed to have been abandoned).

Through this example, however, I would like to stress that the applicability of the risk-based approach has to be considered at the level of individual stakeholders that have to customize the different risks of being exposed to ML and who take actions under the different variations such risks imply. Certainly, different variants of this methodology can be attempted while the most important question to ponder must revolve around the self-referential nature of any system and how self-reference can re-inform (and hopefully improve) parts of a system. For example, whereas the ML-group of this financial institution was originally considering itself as a 'closed-system' it became evident that there was useful information for targeting ML to be found at other departments within the bank. As the MLRO mentioned: 'we really did have a breakthrough when we started cooperating with the marketing department of the bank for the modelling of ML; we used demographic data that they were using and the similarities became evident'. The ML Systems Manager further commented: 'It was like marketing a product to launderers, a product designed with the purpose of identifying them.'

As far as technology and AML is concerned I still remain pessimistic

(despite the somewhat optimistic tone of this section). The interactions between bureaucracy and electreaucracy, the volume of STRs, and the white noise that comes with them, the difficult problem domain of ML, as well as a variety of other problems, all generate uncomfortable dynamics between technology and AML. Despite the improvement mentioned, it is not to be forgotten that a 17 per cent True Positive Rate in automated monitoring implies that from a hundred suspicious transactions that technology generates, only 17 are truly suspicious while 83 remain non-suspicious. Determining whether a flagged transaction (from technology) is suspicious or not requires manual scrutiny by staff members; this is a considerable workload. The problem is unlikely to go away as the nature of modelling ML behaviour is highly complex. As e-transacting becomes more and more prevalent, the difficulties will tend to increase and it is doubtful whether such a high percentage will be sustainable.

EPILOGUE

Even though the task of profiling ML behaviour will remain a core aspect of AML research and practice, it has become evident through the case of Drosia bank that the technological influences to AML do not restrict themselves to profiling technologies alone. A complex nexus of information systems influences the way money laundering analysis teams perform their AML duties. The effects of these interactions propagate across a national AML system and impact on the functioning of the FIU that is burdened with receiving an increasingly larger volume of STRs. Useful information turns to white noise and an already difficult problem area like AML becomes harder to manage.

While the introduction of the risk-based approach has undoubtedly been an interesting regulatory step, the practical side to its implementation is still at a primordial state. The elusive concept of risk, along with its intrinsic paradoxes, creates a level of ambiguity that is reflected at the difficulties of auditing any such risk-based approach.

A large part of this book has been dedicated to the theoretical development of systems theory for the purpose of establishing an academic research programme for the domain of anti-money laundering, including the deconstruction of the risk-based approach through systems theory. While there is indeed a pre-existing wealth of useful research, its common theoretical ground is virtually non-existent. Such research is usually based on frameworks with limited applicability or, quite often, on no frameworks at all, thus resorting to a purely narrative/descriptive approach.

It is at least in this author's contention that systems theory can act as a unifying theory for AML research and practice. It can assist in advancing the various social, economic, political, legal and technological research areas of AML, as well as in facilitating communication amongst academics and practitioners. As an interdisciplinary theory, systems theory is well placed to fulfil this purpose, especially when the domain of application (that is, AML) is interdisciplinary in itself.

Notes

2. INTRODUCTION TO ANTI-MONEY LAUNDERING

1. Hawala is an underground scheme of moving money and is solely based on trust. A customer that seeks to transfer money to a person in another city or country, approaches a Hawala broker (also known as *hawaladar*) and gives the broker the sum of money to be transferred (plus a small commission). The broker communicates with his counterpart Hawala-broker in the city/country and the counterpart arranges for the payment. The Hawala brokers settle the debt at a later moment in time.
2. The extent to which money laundering can create economic instability is very difficult to establish. Catherine England suggests that there are several cases where Gresham's law on 'bad money drives out good money' is not valid. Also, there is a very dubious connection between the underground and the 'upperground' economy and there have been several occasions where legitimate businesses were funded by criminal money.
3. The recognition of the FATF came in the Commission on Narcotic Drugs resolution 5 (XXXIX) of 24 April 1996.
4. The comment from Professor Arlacchi on the effects of globalization came at a panel discussion held at the United Nations, New York, on 10 June 1998, titled: 'Attacking the Profits of Crime: Drugs, Money and Laundering'. The title of Professor Arlacchi's speech was 'The Need for a Global Attack on Money Laundering'.
5. The Egmont Group is an important transnational organization linking various Financial Intelligence Units around the world. Based on a series of questions submitted to the Egmont Group by the author, the Secretariat of the group was kind enough to reply to a few issues regarding the group's efforts in expanding participation and contributing to the world of AML/ATF. Some highlights are presented here from those replies:

   The Egmont Group participates through its different representatives at the typologies exercises of the FATF and different FATF Style Regional Bodies (FSRBs). The FATF since 2008 additionally has a standing invitation to participate in all Egmont Group Operational Working Group (OpWG) meetings where typologies and operational matters are discussed. The Egmont Group also invites FSRBs to participate in OpWG meetings. Typologies, best practices and possible counter measures are discussed during OpWG meetings. There are different types of FIUs with different types of powers that are members of the Egmont Group. These members may have their own specific strategies on how to counter ML/TF in their jurisdictions. In accordance with FATF recommendation 26, FIUs are recommended to provide feedback to reporting entities and publicize year reports that may include typologies as to instruct and sensitize particular financial and other designated sectors to the dangers of ML/TF. Not all Egmont Group members are independent nation states (Aruba-Netherlands Antilles-Bermuda and some other island nations are cases in point). The Egmont Group Outreach Working Group (OWG) maintains a matrix of jurisdictions that are still not members of the Egmont Group and evaluates the progress of these jurisdictions at each Egmont Group meeting. Jurisdictions are at different levels of establishing an operational FIU in Egmont Group terms. The data is not always precise due to the mere fact that conditions are evolving constantly.

6. By its resolution 55/25 of 15 November 2000, the General Assembly adopted the United Nations Convention against Transnational Organized Crime. In accordance with Article 38, Annex 1 of the aforementioned resolution, the United Nations Convention against Transnational Organized Crime entered into force on 29 September 2003.
7. In the 'Customer Due Diligence' work of the Basel Committee, risk is categorized in four categories: reputational, operational, legal, and concentration risk. Reputational risk is portrayed as the potential that adverse publicity regarding a bank's business practices and associations, whether accurate or not, will cause a loss of confidence in the integrity of the institution. Operational risk (which becomes more elaborate in Basel II), is the risk of direct or indirect loss resulting from inadequate or failed internal processes, systems or events. Legal risk essentially refers to the possibility of lawsuits disrupting the operations of a bank. Banks may become subject to lawsuits resulting from a failure to observe mandatory KYC standards. Finally, concentration risk refers to banks that are not able to identify credit concentrations in order to set limits to restrict the banks' exposures to single borrowers. Essential elements of a KYC policy that are analyzed in the paper are customer acceptance policy, customer identification (including general issues and specific issues like those for trust, nominee and fiduciary accounts, corporate vehicles, introduced business, politically exposed persons, non-face-to-face customers), ongoing monitoring of accounts and transactions, risk management. KYC guidance from the Basel Committee has been contained in three papers: The Prevention of Criminal use of the Banking System for the Purpose of ML 1998, The 1997 Core Principles for Effective Banking Supervision and the 1999 Core Principles Methodology.
8. There are three ways to exchange information: a) The Mutual Legal Assistance (MLA) where evidence is transmitted that can be used for prosecution and judicial procedures, b) Communication between the FIUs for exchanging intelligence that might lead to evidence, based on a memoranda of understanding (MoU), established by the Egmont Group, c) The supervisory channel where information is mostly communicated for supervisory purposes, specific assets or liability accounts because of risk and reputation concerns (for example politically exposed persons). The three channels are of course complementary and there is a need to coordinate between interested governmental bodies within a jurisdiction, and of course across national boundaries.
9. In the EU Directive of 1991, Article 12 made clear that 'Member States shall ensure that the provisions of this Directive are extended in whole or in part to professions and to categories of undertakings, other than the credit and financial institutions referred to in Article 1, which engage in activities which are particularly likely to be used for money-laundering purposes'. However, what is severely problematic in such a statement is that the professions that are potential avenues for money laundering are not explicitly defined. Furthermore, the feasibility of actually including several professions for the purposes of combating ML and then having those responsible for being alert to ML, is something that must seriously be taken under consideration. For example, how feasible would it be to have all the jewellery shops (or auction houses) be alert for the FATF blacklist? The evolution of this regulatory response speaks for itself. Even though a number of professions have now been included and are considered to be part of AML, it remains highly questionable whether they are vigilant of ML instances or whether they simply constitute another layer of bureaucracy.

3. ON SYSTEMS THEORY

1. The idea behind holism is one that carries a wide number of paradoxes as well. Whenever the words 'holistic approach' appear in other texts, the reader should always keep in mind that there is no such thing as a 'holistic approach'. The word 'approach' automatically includes a distinction between what is observed, and what is – by necessity – left unobserved. This necessity is imposed whenever there is an observer.

2. It is interesting enough to see how the concept of emergence is found in other disciplines. In artificial intelligence, the analogy is quite straightforward and there is a belief that it is not the several parts of the system that create the intelligence but it is the interaction between them that creates the interesting behaviour. This may lead us to consider the AI system at a macro-level, assembled by its subsystems. There is however a considerable difference regarding the use of the interactivity between different elements and the projected emergence (a rather elusive emergence indeed). The problem remains that the interaction is programmed in a sequence of algorithmic representations that guide the interactions between the different systems and the interaction by itself is not an intrinsic property of the elemental complexity but a set of guided rules for creating the difference. The difference between logical or biological intelligence is therefore often ignored and misplaced. Angell, I. (1993) 'Intelligence: logical or biological', *Communications of the ACM*, **36**(7), 15–16 & 119.
3. In game theory, it is considered that the ability to generate random behaviour is critical. However it is viewed that as individuals are poor at behaving randomly, that the randomness mechanism in game theory can be found not in individual players but in their interaction. West, R. & Lebiere, C. (2001), 'Simple games as dynamic, coupled systems: randomness and other emergent properties', *Journal of Cognitive Systems Research*, **1**(4), 221–39.
4. A triality is defined here to be the existence of a three-party duality (system-boundary, boundary-environment).
5. While talking about a daunting infinite regression (that progresses!) in the construction of any system, one cannot but associate this to one of the most crucial observations on the problems of philosophy and theory construction that have been discussed by Nietzsche (amongst others); that is, a description about something that exists in its opposite (truth in error, and in this scenario, regression in progression), a matter that cannot clearly be resolved but one that could possibly – I would add – be a testament to the process of systemic differentiation about the ontological impossibility of a system in isolation (that is, without an environment). Nietzsche, F. (1977), *Logic, Epistemology, Metaphysics. A Nietzsche Reader*, London: Penguin Books.
6. The first time I heard the example of the human brain and the threshold of emergence for cognition was when I was studying Physics at the University of Crete. I attribute this to Professor Gregory Psaltakis who described the example in his course on Quantum Physics.
7. Sooner or later, the quest for entropy and negentropy has an end and entropy catches up thus leading to the not so comforting thought of the maximum state of entropy (being systemic death). Particularly for cognitive systems such as human beings and insofar as the philosophical quests include pursuits of this level, a common argument (from Martin Heidegger) would be that the purpose of all human life, all of its manifestations and archetypal forms of construction are self-referential (created from and for the human) so that the human mind is constantly preoccupied and able to keep straying away from its cognitive processes that conceptualize the thought of the maximum entropy. Heidegger, M. (1994), *Basic questions of philosophy: selected 'problems' of 'logic'*, Bloomington: Indiana University Press.
8. It is indeed important to offer some reflections on complexity and the elements that constitute a system. The problem of atomism may rise here when one ponders the question of the elements that can be further dissolved. And indeed, one would be right to observe that there is little that can forbid us to go down that road, that is, to say that if we view elements at a microscopic level then we will see that those in their own turn are highly complex and therefore what constitutes the unity of an element is something highly debatable and frail. As Luhmann observed (p. 24–25 in *Social Systems*), 'whether the unity of an element should be explained as emergence from below or as constitution from above seems to be a matter of theoretical dispute. . . we opt decisively for the latter'. And not without reason, one could add; elements are elements (this is an ontological issue) only for the system that employs, registers, and functions through them.

9. The reproduction of the Klein bottle was done with the Mathematica software package by Wolfram Research.
10. The reader can look at a visualization example with digits at: http://people.cs.uchicago.edu/~dinoj/vis/digits/index.html
11. In the scenario where information processing can also occur between two abstractions it becomes even more evident that input is internalized. In the scenario of the addition between two numbers, self-reference implies that the technical system will need to refer to itself and the abstraction within it for the addition to be carried out. This further separates an esoteric system/environment relationship between one abstraction (one number) and another abstraction (another number). One may serve as a system and one as an environment while a third abstraction (an operator like +) becomes the function with which both system and environment are engaged into a structural coupling and further produce the output of the result (which in its own turn may be further internalized for further information processing).

4. THE CASE STUDY OF DROSIA BANK

1. Querying databases always implies some sort of profiling (simple or complex). In this scenario, the Automated Centre for Transaction Recording would computationally execute a query that would match several fields in different accounts. For instance, if a person had the same last and first name, then that would be flagged out as a potential positive match and the case would be further investigated so that multiple accounts could be united into one number in the POSEIDON system.
2. This is not to say that centralization is preferable to decentralization. Depending on the operations that are employed from the perspective of an organization, the degree of centralizing or decentralizing functional operations is difficult to examine and it remains highly contextual.
3. To see the corruption timeline for the government of Belarus, the reader may refer to: http://report.globalintegrity.org/Belarus/2008/timeline
4. A simple example of the problems faced by UPS in handling the multilingual challenge in an information system setting can be found at: http://www.cio.com/archive/011501/et.html

5. SYSTEMS THEORY – A THEORY FOR AML

1. With the introduction of discussion paper DP22 by the Financial Services Authority (FSA), entitled *Reducing Money Laundering Risk – Know your customer and anti-money laundering monitoring*, technology adoption for AML was on the table for discussion. Even though many financial institutions had already started looking into automated technological solutions for dealing with AML, this FSA initiative institutionalised the use of profiling technology considerably.
2. In the UK, a total of 500 staff work for the 57 LEAs (!) have to cope with the forwarded STRs.
3. This is an adapted version of the table presented here in order to indicate only *system* and *code*.
4. The practice of blacklisting individuals particularly for the financing of terrorism has received some considerable criticism lately from the European Commission where it was stated that the 'procedures used by the UN Security Council for blacklisting individuals are 'totally arbitrary and have no credibility whatsoever': http://assembly.coe.int/ASP/Press/StopPressView.asp?ID=1972.

5. The Australian FIU even congratulated the UK FIU (former NCIS, now SOCA) upon an increase in the number of STRs received year after year.
6. A link to the Japanese FIU for the latest available report: http://www.fsa.go.jp/en/index.html.

6. THE RISK-BASED APPROACH AND A RISK-BASED DATA-MINING APPLICATION

1. Part of this chapter dealing with the risk-based approach has previously appeared in print as: Demetis, D and Angell, I (2007), 'The risk-based approach to Anti-Money Laundering: representation, paradox, and the 3rd Directive', *Journal of Money Laundering Control*, **10** (4).
2. In November 2007, two computer discs holding the personal details of all families in the UK with a child under the age of 16 went missing. These discs contained names, addresses, date of birth, national insurance numbers, and bank details of 25 million people. Chancellor Alistair Darling urged people to monitor their bank accounts for unusual activity while the value of the discs to criminals was estimated around £1.5bn.

References

9/11Commission (2004), 'The 9/11 Commission Report', available at http://www.9-11commission.gov/.

Angell, I. (1993), 'Intelligence: logical or biological', *Communications of the ACM*, **36** (7), 15–16 & 119.

Angell, I. (2000), *The New Barbarian Manifesto: How to Survive the Information Age*, London: Kogan Page.

Angell, I. (2008), 'As I see it: enclosing identity', *Identity in the Information Society*, **1** (1), 23–37.

Angell, I. & Demetis, D. (2005), 'Systems thinking about Anti-Money-Laundering: considering the Greek case', *Journal of Money Laundering Control*, **8** (3), 271–84.

Angell, I.O. & Smithson, S. (1991), *Information Systems Management*, London: Macmillan.

Arbib, M. & Cornelis, A. (1981), 'The role of system theory in the social sciences: an interview', *Journal of Social Biological Structures*, **4**, 375–86.

Ashby, W.R. (1958), *An Introduction to Cybernetics*, London: Chapman and Hall.

Avgerou, C. (2000), 'Information systems: what sort of science is it?' *Omega: The International Journal of Management Science*, **28** (5), 567–79.

Basel (1988), 'Statement on prevention of criminal use of the banking system for the purpose of money-laundering', available at http://www.bis.org/publ/bcbsc137.pdf.

Basel (2001), 'Customer due diligence for banks', Basel Committee on Banking Supervision.

Basel (2002), 'Sharing of financial records between jurisdictions in connection with the fight against terrorist financing', Basel Committee on Banking Supervision.

Basel (2003a), 'Consolidated KYC Risk Management', Basel Committee on Banking Supervision.

Basel (2003b), 'Shell banks and booking offices', Basel Committee on Banking Supervision.

Basel (2004), 'Basel II: international convergence of capital measurement

and capital standards: a revised framework', available at http://www.bis.org/publ/bcbs107.htm.
Bateson, G. (1972), *Steps to an Ecology of Mind*, New York: Ballantine Books.
Bausch, K. (2002), 'Roots and Branches: a brief, picaresque, personal history of Systems Theory', *Systems Research and Behavioral Science*, **19** (5), 417–28.
BBC (2006), 'London bombs cost just hundreds', available at http://news.bbc.co.uk/2/hi/uk_news/4576346.stm.
Bertalanffy, L. (1969), *General System Theory*, New York: George Braziller, Inc.
Canhoto, A. & Backhouse, J. (2007), 'Profiling under conditions of ambiguity – an application in the financial services industry', *Journal of Retailing and Consumer Services*, **14**, 408–19.
Checkland, P. (1985), 'From optimizing to learning: a development of Systems Thinking for the 1990s', *Journal of the Operational Research Society*, **36** (9), 757–67.
Christin, I. (1983), 'Financial Systems: a few theoretical and algebraic considerations for their modeling', *Mathematical Social Sciences*, **6** (2), 171–93.
Coward, L.A. (2005), *A System Architecture Approach to the Brain: From Neurons to Consciousness*, New York: Nova Biomedical Books.
Crotty, M. (1998), *The Foundations of Social Research*, London: SAGE Publications.
CS (2001), *A Model of Best Practice for Combating Money Laundering in the Financial Sector; Economic Paper 43*, Commonwealth Secretariat.
Davies, G. (2002), *A History of Money from Ancient Times to the Present Day*, Cardiff: University of Wales Press.
Demetis, D. (2004), 'The World on Discount', *The Journal of the London School of Economics SU*, **3** (1).
Demetis, D. & Angell, I. (2006), 'AML-related technologies: a systemic risk', *Journal of Money Laundering Control*, **9** (2), 157–72.
Demetis, D.S. (2009), 'Data growth, the new order of information manipulation and consequences for the AML/ATF domains', *Journal of Money Laundering Control*, **12** (4), 353–70.
Demetis, D.S. & Angell, I.O. (2007), 'The risk-based approach to AML: representation, paradox, and the 3rd Directive', *Journal of Money Laundering Control*, **10** (4), 412–28.
Ditton, J. & Brown, R. (1981), 'Why don't they revolt? "Invisible Income" as a neglected dimension of Runciman's relative deprivation thesis', *The British Journal of Sociology*, **32** (4), 521–30.

Duyne, P.V. (1998), 'Money-Laundering: Pavlov's dog and beyond', *The Howard Journal*, **37** (4), 359–74.
Emery, F & Trist, E (1965), *Human Relations*, **18** (1) 21–32.
England, C. (2000), 'Is privately-provided electronic money next?', Institute of Economic Affairs.
EU (1991), Council Directive 91/308/EEC of 10 June 1991 on prevention of the use of the financial system for the purpose of money laundering, available at http://europa.eu.int/scadplus/leg/en/lvb/l24016.htm.
EU (2001), Directive 2001/97/EC of the European Parliament and of the Council of 4 December 2001, available at http://www.europa.eu.int/eur-lex/pri/en/oj/dat/2001/l_344/l_34420011228en00760081.pdf.
EU (2005), Directive of the European Parliament and of the Council on the prevention of the use of the financial system for the purpose of money laundering, and terrorist financing, available at http://europa.eu.int/comm/internal_market/company/financial-crime/index_en.htm.
FATF (1990), The Forty Recommendations of the Financial Action Task Force on Money Laundering.
FATF (2002), Guidance for Financial Institutions in Detecting Terrorist Financing, available at http://www.fatf-gafi.org/datao-ecd/39/21/34033955.pdf.
FATF (2003), 'What is Money Laundering?', available at http://www1.oecd.org/fatf/MLaundering_en.htm.
FIDIS (2009), D17.1 Modelling New Forms of Identities: Applicability of the Model Based on Virtual Persons.
Fowler, G. & Qin, J. (2007), 'QQ: China's New Coin of the Realm?', available at http://online.wsj.com/public/article/SB117519670114653518-FR_svDHxRtxkvNmGwwpouq_hl2g_20080329.html.
GATE (2008), The GATE-Project on Anti-Money Laundering and Terrorist Financing (funded by the European Commission on Security Research).
Germana, J. (2001), 'Emergent properties: a fundamental postulate of classical systems theory in schematic representation', *Systems Research and Behavioral Science*, **18** (6), 565–68.
Geyer, F. (2002), 'The march of self-reference', *Kybernetes*, **31** (7), 1021–42.
Gilmore, W. (1993), 'Money laundering: the international aspect', *Public Policy*, **1** (2).
Gilmore, W. (1999), *Dirty Money: The Evolution of Money Laundering Counter-Measures*, Strasbourg: Council of Europe Press.
Glass, N. (1996), 'Chaos, non-linear systems and day-to-day management', *European Management Journal*, **14** (1), 98–106.
Gleick, J. (1988), *Chaos: Making a New Science*, New York: Penguin.

Goodman, N. (1976), *Languages of Art: An Approach to a Theory of Symbols*, Indianapolis: Hackett Publishing Company.
Granville, J. (2003), 'Dot.*Con*: the dangers of cyber crime and a call for proactive solutions', *Australian Journal of Politics and History*, **49** (1), 102–9.
Greenberg, L.T. & Goodman, S.E. (1996), 'Is Big Brother Hanging by His Bootstraps?', *Communications of the ACM*, **39** (7).
Hayek (1978), *Denationalisation of Money – The Argument Refined*, London: Institute of Economic Affairs.
Heidegger, M. (1994), *Basic Questions of Philosophy: Selected* '*Problems*' *of* '*Logic*', Bloomington: Indiana University Press.
Hilborn, R. (1994), 'Predictability: does the flap of a butterfly's wings in Brazil set off a tornado in Texas? – Lorenz's talk to the American Association for the Advancement of Science', *Chaos and Nonlinear Dynamics*, Oxford: Oxford University Press.
Holder, W. (2003), 'The International Monetary Funds involvement in combating money laundering and the financing of terrorism', *Journal of Money Laundering Control*, **6** (4), 383–7.
Hugel, P. & Kelly, J. (2002), 'Internet gambling, credit cards and money laundering', *Journal of Money Laundering Control*, **6** (1), 57–65.
Johnson, J. (2001), 'In pursuit of dirty money: identifying weaknesses in the global financial system', *Journal of Money Laundering Control*, **5** (2), 122–32.
Johnson, J. (2003), 'Repairing legitimacy after blacklisting by the Financial Action Task Force', *Journal of Money Laundering Control*, **7** (1).
Johnson, J. & Lim, D. (2002), 'Money laundering: has the Financial Action Task Force made a difference?', *Journal of Financial Crime*, **10** (1), 7–22.
Kallinikos, J. (2005a), 'Information out of information: on the self-referential dynamics of information growth', *Information Technology and People*, **19** (1), 98–115.
Kallinikos, J. (2005b), 'The order of technology: complexity and control in a connected world', *Information and Organization*, **15**, 185–202.
Kallinikos, J. (2006), *The Consequences of Information: Institutional Implications of Technological Change*, Cheltenham, UK and Northampton, Mass.: Edward Elgar.
Korzybski, A. (1948), *Science and Sanity: An Introduction to Non-Aristotelian Systems and General Semantics*, Lakeville, Conn.: International Non-Aristotelian Library Pub. Co.; Institute of General Semantics.
KPMG (2003), Money Laundering: Review of the Reporting System.
Lee, A. (2003), 'Systems Thinking, Design Science and Paradigms',

available at http://saturn.vcu.edu/~aslee/ICIM-keynote-2000/ICIM-keynote-2000.htm.
Lilley, P. (2000), *Dirty Dealing*, London: Kogan Page.
Lilley, P. (2006), 'Black-listing process', available at http://www.dirtydealing.net.
Lin, Y. (1988), 'Can the world be studied in the viewpoint of systems?', *Mathematical Computer Modelling*, **11**, 738–42.
Luhmann, N. (1990), *Essays on Self Reference*, New York: Columbia University Press.
Luhmann, N. (1993), *Risk: A Sociological Theory*, New Brunswick: Transaction Publishers.
Luhmann, N. (1995), *Social Systems*, Stanford, Calif.: Stanford University Press.
Luhmann, N. (2000a), *Art as a Social System*, Stanford: Stanford University Press.
Luhmann, N. (2000b), *The Reality of the Mass Media*, Cambridge: Polity Press.
Luhmann, N. (2002), *Theories of Distinction: Redescribing the Descriptions of Modernity*, Stanford: Stanford University Press.
Luhmann, N. (2004), *Law as a Social System*, Oxford; New York: Oxford University Press.
Luhmann, N. (2005), 'The concept of Autopoiesis', in Clegg, S. & Stablein, R. (eds), *Niklas Luhmann and Organization Studies*, Copenhagen: Liber & Copenhagen Business School Press.
Maguire, S. & McKelvey, B. (1999), 'Special issue on complexity and management: where are we?', *Emergence*, **1** (2).
Masson, P. (2001), Globalization: facts and figures', IMF Policy Discussion Paper.
Maturana, H. & Varela, F. (1998), *The Tree of Knowledge: The Biological Roots of Human Understanding*, Boston & London: Shambhala.
Mayr, E. (2000), *What Evolution Is*, New York: Basic Books.
McCarthy, C. (2006), 'Principles-based regulation – what does it mean for the industry?', available at http://www.fsa.gov.uk/pages/Library/Communication/Speeches/2006/1031_cm.shtml.
McDonell, R. (1998), 'Money laundering methodologies and international and regional counter-measures', paper presented at the Gambling, Technology and Society: Regulatory Challenges for the 21st Century, Sydney 7–8 May.
Mitleton-Kelly, E. (2003), *Complex Systems and Evolutionary Perspectives on Organizations: The Application of Complexity Theory to Organizations*, Oxford: Pergamon Press.

Moeller, H.-G. (2006), *Luhmann Explained*, Peru, Illinois: Carus Publishing Company.
Mohamed, S. (2002), 'Legal instruments to combat money laundering in the EU financial market', *Journal of Money Laundering Control*, **6** (1), 66–79.
Naylor, R.T. (1994), *Hot Money and the Politics of Debt*, Montreal, Quebec: Black Rose Books.
Nietzsche, F. (1977), 'Logic, Epistemology, Metaphysics', in *A Nietzsche Reader*, London: Penguin Books.
OFAC (2007), 'Terrorist Assets Report', available at http://www.treas.gov/offices/enforcement/ofac/reports/tar2007.pdf.
Parkman, T. & Peeling, G. (2007), *Countering Terrorist Finance*, Aldershot, UK: Gower Publishing.
Philippsohn, S. (2001), 'Money laundering on the Internet', *Computers & Security*, **20**, 485–90.
Pinter, H. (2005), 'Art, Truth and Politics', available at http://nobelprize.org/literature/laureates/2005/pinter-lecture.html.
Popper, K. (2002), *The Logic of Scientific Discovery*, Abingdon, Oxon: Routledge.
Price, A. (2002), 'Anti-Money Laundering: reconsidering the risks', *Ernst & Young Monitor Magazine (Strategic Issues for Financial Services Executives)*.
Quirk, P. (1996), 'Macroeconomic implications of money laundering', *IMF Working Paper*, WP/96/66.
Ramos-Martin, J. (2003), 'Empiricism in ecological economics: a perspective from complex systems theory', *Ecological Economics*, **46** (3), 387–98.
Rider, B. (2003), editorial: 'Who to trust!', *Journal of Money Laundering Control*, **6** (4), 299–300.
Robinson, J. (1998), *The Laundrymen*, London: Simon & Schuster UK.
Rossbach, S. (1993), *The Author's Care of Himself: On Friedrich Nietzche, Michel Foucault, and Niklas Luhmann*, Florence: European University Institute.
Roule, T. & Salak, M. (2003), 'The anti-money laundering regime in the Republic of Nauru', *Journal of Money Laundering Control*, **7** (1), 75–83.
Scholte, J. (1997), 'Global capitalism and the State', *International Affairs*, **73** (3), 427–52.
Scott, B. (2004), 'Second-order cybernetics: an historical introduction', *Kybernetes*, **33** (9), 1365–78.
Searle, J. (1995), *The Construction of Social Reality*, London: Penguin Books.

Selgin, G. (1994), 'On ensuring the acceptability of a new fiat money', *Journal of Money, Credit and Banking*, **26** (4), 808–26.
Skyttner, L. (1998), 'The future of Systems Thinking', *Systemic Practice and Action Research*, **11** (2).
Spiegel (2007), 'Sweden Opens Virtual Embassy in Second Life', available at http://www.spiegel.de/international/0,1518,463073,00.html.
Spotlight (2006), 'New approaches to fighting money-laundering', available at http://www.spotlight.uk.com, London School of Economics.
Tanzi, V. (1996), 'Money laundering and the international financial system', IMF Working Paper, WP/96/55.
Tanzi, V. (1999), 'Uses and abuses of estimates of the underground economy', *The Economic Journal*, **109**, 338–47.
Tupman, W.A. (2009), 'Ten myths about terrorist financing', *Journal of Money Laundering Control*, **12** (2), 189–205.
UN (1988), 'United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances', available at http://www.incb.org/e/conv/1988/index.htm.
UN (1998a), 'Attacking the profits of crime: drugs, money and laundering. New York', available at http://www.un.org/ga/20special/.
UN (1998b), Political Declaration and Action Plan against Money Laundering.
UN (1998c), Political Declaration on Global Drug Control at the UN General Assembly – Twentieth Special Session, available at http://www.un.org/ga/20special/poldecla.htm.
UN (2000), The United Nations Convention against Transnational Organized Crime, available at http://www.unodc.org/unodc/en/crime_cicp_convention.html.
Von Foerster, H. (1951), *Cybernetics, Circular Causal and Feedback Mechanisms in Biological and Social Systems: Transactions*, New York: Josiah Macy, Jr. Foundation.
Von Foerster, H. & Josiah Macy, Jr. Foundation. (1950), Transactions of the Conference, New York: Josiah Macy, Jr. Foundation.
Von Foerster, H.M., Zopf, G.W. & United States Office of Naval Research (1962), *Principles of Self-Organization: Transactions*, New York: Symposium Publications, Pergamon Press.
Walker, J. (1998), 'Modelling Global Money Laundering Flows', available at http://members.ozemail.com.au/~born1820/mlmethod.htm.
Walker, J. (1999), 'How big is global money laundering?', *Journal of Money Laundering Control*, **3** (1).
West, R. & Lebiere, C. (2001), 'Simple games as dynamic, coupled systems: randomness and other emergent properties', *Journal of Cognitive Systems Research*, **1**(4), 221–39.

Whitley, E. (2006), Research essays in Information Systems: lecture at the London School of Economics, London.

WorldBank (2001), 'World Development Report: Growth, Inequality and Poverty', available at http://www.worldbank.org/poverty/wdrpoverty/report/, The World Bank.

Xu, L. (2000), 'The contribution of systems science to information systems research', *Systems Research and Behavioral Science*, **17** (2), 105–16.

Yoshida, J. (2001), 'Euro bank notes to embed RFID chips by 2005', available at http://www.eetimes.com/story/OEG20011219S0016.

Zemke, R. (2001), 'Systems thinking: looking at how systems really work can be enlightening – or a wake-up call', *Journal of Training*, **38** (2).

Index