THE LONDON SCHOOL OF ECONOMICS AND POLITICAL SCIENCE

A Systems Theoretical approach for Anti-Money Laundering informed by a Case Study in a Greek Financial Institution:

Self-reference, AML, its systemic constitution and technological consequences

Dionysios S. Demetis

http://www.demetis.com

Department of Management
Information Systems and Innovation Group
London School of Economics and Political Science
Houghton Street, London WC2A 2AE, UK

Dissertation submitted in fulfilment of the requirements for the award of the degree of Doctor of Philosophy

ProQuest LLC
789 East Eisenhower Parkway
P.O. Box 1346
Ann Arbor, MI 48106-1346

Abstract

This dissertation constitutes a systems theoretical analysis of Anti-Money Laundering that dismisses the projected ideals of holism and delves into the core of Systems Theory (ST) in the tradition of second-order cybernetics. This theoretical approach of ST is appropriated in order to describe the domain of Anti-Money Laundering (AML) as a system in itself and at the same time examine the consequences that technology comes to play within the system of AML. While the contemporary phenomenon of AML has been reduced mostly into a set of technological consequences from profiling technologies (technologies that attempt within financial institutions to model and simulate money-laundering behaviour for the generation of suspicious transactions), this dissertation takes a different approach. Instead of focusing at profiling technologies that are believed to be the core technological artefacts that influence AML within financial institutions, this dissertation examines a variety of information systems and their interplay and describes through empirical findings the multitude of interactions that are technologically supported and that construct a much more complex picture of dealing with AML and thereby influencing how money-laundering is perceived. The empirical findings supporting the theoretical treatise come from a longitudinal case study of a Greek financial institution where a systematic examination takes place regarding a variety of information systems that may affect AML within the bank. Beyond isolated interferences of information systems to AML, their interrelations are further examined in order to reflect on the emergent complexity that often distorts cause-and-effect AML manipulations. The theoretical contributions put forward, constitute a systems theoretical application and an expansion of technological/systemic interferences, while the practical contributions to AML cover broader systems-theoretical reflections on the domain, technological integration within financial institutions for targeting ML, feedback relations between financial institutions and Financial Intelligence Units, as well as the systemic consequences for the newly implemented risk-based approach.

Red rose of the wind and of the fate,
You have lingered in my memories, like a heavy rhythm
Rose of the night, you have passed, tempest of a red veil
Tempest of the sea ... The world is simple.

George Seferis
Athens, 1929

To Professor Ian O. Angell

Table of Contents

List of Tables & Figures

Acknowledgements

The reader may skip this (hopefully enjoyable) section as I intend to make no exceptions in thanking wholeheartedly the good number of people that I have met at the London School of Economics and elsewhere, and who have supported me throughout my research in one way or another. I would like to thank (in no particular order):

Anna Palamidi, for always being there for me, and for continuing to do so,
Christoforos Moutafis, for making me laugh while being severely injured in Cambridge during the French festival, for accepting to perform as the best 'koumparomaterial' ever, and for not going to these pretentious formal balls,
Sarah Emery, for being the best boss and friend one could ever have,
Ashutosh Khanna, for our unique strolls up and down Tower I, and the discussions,
James Backhouse, for Spotlight and for trusting me with the classes of his Security course within our IS integrity group,
Bernard Dyer, for the stories, the ants, and our endless collaboration,
Antonio Cordella, for the Stella-Shandy, his Italian accent, and Sapori,
Chrysanthi Avgerou, for our interesting conversations and for sending me to MCIS,
Cheryl Edwardes, for her giggle and always sharp-commentary,
Magda Hercheui, for her energy, particularly on the dance-floor,
Katerina Voutsina, for being one of my best friends despite her Kefallonia-origin,
Jonathan Ezer, for discussing, discussing, and ... eventually publishing together,
Joanna Chini, for staying alive after choosing the dangerous sport of kayaking on the Thames,
Avgousta Kyriakidou, for remaining calm on an unprecedented number of occasions,
Daniel Osei-Joehene, for his early advice about making money that I failed to follow, and so I believe did he, in light of too many philosophical interests,
Dominique Lazanski, for the help and the music,
Federico Iannacci, for our interesting discussions on national-corruption and more,
Hemini Mehta, for being so cute and kind, and not changed by the BBC,

Prodromos Tsiavos, for keeping my Eric Cartman quote and the Naples tragic ornament,

Spiro Samonas, for our common photographic interests at the Student Support Desk,

Shirin Madon, for I would prefer no one else to give me the good news of my PhD upgrade in the sweetest possible way, (& she plays the piano!),

Jannis Kallinikos, for Greek poetry on Kalvos, for introducing me to Luhmann, our chapter in his book, and the 'what is reality' quote,

Frank Land, for accepting my invitation three times in a row to give a fantastic set of lectures to our students,

Carsten Sorensen, for without him I would have forgotten what it would be like to be a computer geek, for the music, and for the crucial advice in life-changing moments,

Steve Smithson, for trusting me with the dissertation classes, letting me organise the weekly seminars at the LSE for our MSc students, and our occasional cigarette down Tower I,

Maha Shaikh, for one only knows what trust really means with Maha as a friend,

Everyone who is not on this list, for memory is often week and space limited,

My Students at LSE, for reviving my brain cells in every single class,

Jose-Carlos Mariategui, for the satanic laughter and for founding Nepheli Ltd,

My Parents, for without them my ontological question would not exist,

My PhD supervisor, Professor Ian Oakley Angell,

for accepting me as his PhD student,

for putting yellow marks all over my written documents,

marks that gradually turned purple,

for the right-o quote, (after the kettle has been set for tea)

for teaching me how to balance the Force,

for our always heated discussions and debates,

for not allowing me to win over one single argument, and for saying to me: "All in good time, balance the Force, learn you shall".

And for everything else that spacetime and words cannot encapsulate.

Right-o.

Prologue

As any dissertation contains and confronts an antithesis, this one cannot but wholeheartedly embrace its own. The antithesis I speak of has been the challenge to combine, confront and reflect on somewhat different levels: that of philosophical abstraction represented by theory, and that of specificity represented by the somewhat more pragmatic domain of Anti-Money Laundering (AML). In dealing with deep philosophical issues and confronting theoretical challenges I have found tremendous pleasure in choosing Systems Theory as the theory that would guide this research, and unavoidably, a theory that has for myself constituted an entire paradigm of thinking about any problem. At the same time, I have found a great deal of pleasure in dealing with the domain of AML as a pragmatic problem affecting financial institutions worldwide.

In dealing with AML, I have come to witness its evolution throughout a number of years and under a number of capacities. First as a young researcher into the problem domain by examining a few financial institutions, then as a PhD student in dealing with a single institution for a long period of time, then as an associate and author for two European Commission funded projects on AML (Spotlight[1] and Gate[2]) and various other publications, and most recently as an independent AML-expert giving consultation seminars in a number of financial institutions and organisations in Europe and the Middle East. Many things have changed over these years, even though global evidence that the AML domain is becoming more effective in dealing with the problem domain is consistently missing. One thing is certain, for those observing the problem itself: its complexity increases and so is the complexity of AML.

In discovering Systems Theory during my Masters degree in Information Systems at the London School of Economics when Professor Ian Angell – later on to become my PhD supervisor – outlined the fundamental constructs of the theory, I have come to realise that there is something terribly appealing in that theory. It was much later that I discovered how my first Degree in Physics would conceptually help me tackle systems theoretical concepts in dealing with systems of greater complexity and/or descriptive variation. Within the multitude of theoretical constructs in existence, I cannot think of one that could surpass the theoretical richness and depth of examination that Systems Theory can offer.

This dissertation has been the product of a long intellectual journey that now strangely seems to have ended, or rather has reached a new beginning (one always keeps the prologue for the end). I hope that the reader finds this pleasure on both fronts, those of theory and practice, but more importantly in their combination.

---

[1] http://www.spotlight.uk.com
[2] http://www.exodus.gr/gate

Chapter I: Introduction

Anti-Money Laundering has become an important contemporary phenomenon that has generated a great deal of attention, predominantly in the past two decades. While the net of stakeholders involved in AML has expanded due to regulatory initiatives, financial institutions remain at the forefront of the fight against money-laundering. Consequently, the study of how financial institutions deal with this important problem domain remains crucial. Financial institutions, however, do not exist in a void. They are part of a complex socio-political and economic arena that is advancing in particularly structured ways, but with unstructured consequences.

Whatever modernity may come to mean in this regard, modern society may be characterised by a number of attributes, although it is evident that technology has come to occupy a central role in this self-proclaimed modernity. Technology as broadly understood has of course little to do with both the wider study of information systems and the very concept of *systems* as will be developed and analysed in this dissertation. Still, our dependence on technology has increased considerably, and it is becoming evident that a technology that fails to function no longer comes to a halt, but triggers unanticipated effects of possibly catastrophic dimensions. Such catastrophic dimensions not only permeate problem domains like AML, but also, and even worse, they often go unnoticed or they become masked as an operative success by the systems that employ the technological function and all that this implies. Hence, in a large number of fields, society has come to rely on technology functioning, and develops its own structures more and more on the basis of this precondition of reliance.

This technological precondition is not an exception merely within AML. Financial Institutions have always been technologically astute, and have expanded their own 'closed' organisational structures to include technological developments that were viewed as beneficial within their own structures.

The current conditions in the broader AML domain appear therefore to have acquired a highly unstructured complexity - a complexity partly due to the regulatory initiatives that have spawned a myriad of reactions, and partly due to the technological implementations improvised to accommodate and automate aspects of those reactions.

Such complexity is also reinforced by an unrestrained opportunism shown by the software industry that 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. Consequently software has found a vulnerable ground that has resulted in considerable automation with adverse effects for Financial Intelligence Units. Last but not least, the risk-based approach and its introduction with the 3rd Directive has created a multitude of additional ambiguities. Even though the European Union (EU) has rightly taken the step of introducing a more flexible approach in the fight against ML, a series of difficulties and uncertainties have been introduced in how such a risk-based approach should be implemented, and furthermore, how individual institutions and Financial Intelligence Units are to make sense of this newly-born complexity that comes with the very elusive nature of risk. Typical stances within these new difficulties sourcing from the risk-based approach can be found not only in financial institutions but also in the regulators. In the UK for example, the Financial Services Authority has scrapped the detailed AML guide and introduced high-level principles in line with the risk-based approach. At the same time, however, checking compliance becomes compromised. How will risk-based supervision be put into practice when the internal document that is the basis of checks by the FSA is labyrinthine? Even the Chairman of the FSA accepts this to be a problem, noting: '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'[3].

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. Such a strong assertion is not carried out here with the purpose of overemphasizing the problems. This section merely remains a preface to the academic discussion that follows. The reality however also remains, that feedback between FIUs and financial institutions is at a primordial state, interoperability issues are barely considered, while stakeholder fragmentation as well as the sharing of intelligence – even at an anonymized form that would not jeopardise data protection and privacy issues – is left unattended.

[3] http://www.fsa.gov.uk/pages/Library/Communication/Speeches/2006/1031_cm.shtml

Within this dynamic, between regulatory initiatives and technological development (even though development here should not be taken to imply improvement in any regard), the domain of AML is considerably reconstructed.

Much like a biological organism that encodes its own survival and evolution within a double-helix of genetic code, the Anti-Money Laundering System becomes structurally coupled with the system of technology with which it co-evolves. Examination of such an interplay implies two things to be considered together: how is AML a system? And also, how is technology a system? Beyond the realm of technology, as commonly perceived, this dissertation seeks to offer an insight (through the empirical data gathered and the analysis put forward) into the broader effects that various information systems have within a financial institution in relation to Anti-Money Laundering. This implies that the commonly perceived technological structures that currently affect ML, those of profiling technologies that attempt to simulate money-laundering behaviour and hence capture suspicious transactions, remain but a single instance of a broader structure of various information systems that have similar (if not more powerful and propagating) effects on AML.

This dissertation seeks to give an answer to the following research questions:

i. What theoretical description can be developed in order to describe the domain of Anti-Money Laundering through the lens of *Systems Theory*?

ii. What is the role that various information systems come to occupy within financial institutions, which in their own turn try to tackle the problem of ML, and how do the complex interactions between various information systems employed affect AML?

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

Chapter III, the methodology chapter, outlines both the basic research principles that guide the research process throughout its stages, and the methodological choices being made, while also seeking to contribute to the broader construction of a methodological process.

Chapter IV presents the key theoretical principles of *Systems Theory* that constitute the foundational basis for developing a further theoretical treatise and for relating systems principles to AML.

Chapter V describes the empirical findings that have sourced from a longitudinal case study carried out in a major financial institution in Greece, and relates the various information systems instances in order to ponder the second research question outlined above.

Chapter VI, the final chapter, analyses and discusses a number of systemically theoretical instances that lead to a description of AML as a *system* (in the systems theoretical sense of the second-order cybernetics tradition). 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. This is followed by an endeavour to extrapolate these observations in order to provide both theoretical and practical contributions.

The dissertation concludes with some final remarks and offers some suggestions for further research.

Chapter II: Literature Review

Chapter Structure

This chapter reviews the literature on anti-money-laundering in four different sections. In this prologue, a brief description of each section follows:

i) Section I tries to deconstruct the problem of defining money-laundering. The problem of definition (besides being a semantic issue) is one of crucial importance. Using 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.

ii) Section II describes the plethora of problems that come into existence when we try to estimate the scale of the money-laundering market. There are reasons to suggest that the market has increased, despite the attempts to estimate it proving highly problematic.

iii) Section III presents the major international initiatives against Money Laundering. As the initiatives are many, and their contents often complicated, an effort is made to present these in a clear chronological order. A brief description follows of the most important initiatives, ending with an attempt to categorize the major contributions.

iv) Section IV describes some features of the global anti-money-laundering arena, which will hopefully provide the reader with a broader perspective of the domain, and will solidify some of the arguments put forward.

Section I: Deconstructing Money-Laundering

What is Money-Laundering?

In order to formulate a definition on what money-laundering (ML hereinafter) is, we must take into consideration the fact that ML is first and foremost a *process* that is dynamic and can therefore change considerably. Furthermore, we must also ponder the question of what the nature of the *money* being laundered actually is. I will commence by examining the latter.

The nature of the laundered money

The way money is used, and perceived of 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 in *commodities* like ivory, leather, gold, etc. Banking these commodities meant storing them in warehouses and keeping track of the exchanges. 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* here 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 'The Social Construction of Reality', Searle (1995) gives a compelling account of how institutional facts are created, and he thoroughly examines the example of money.

Critical in the process of creating institutional facts is the *collective intentionality*[4], which cannot be reduced to an individual's intentionality. As Searle frames it (p.41):

> "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."** (Emphasis added) – (ibid)

Applied to money, this brings us to the realization that without the collective intentional imposition of function on money, *money would not be able to function as such.* Impositions of functionality on money are typically done by institutions that express the aforementioned collective intentionality. These institutions have a status that is not easily contested, disputed or refuted. For instance, central banks can be seen 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 utilisation of money. Such impositions are also carried out in systems like Hawala, 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 'underground'), is as good as money[5].

Most academic-related material that examines the nature of money usually distinguishes three common forms [i.e. (Davies 2002)]:

Commodity money: Gold[6] or other materials.
Contract money: Pieces of paper that promise to pay the bearer in gold.

[4] According to Searle (1995, p.46) 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, a new fact created by human agreement.'
[5] Money here refers to the commonly shared institutional fact that we recognize as legitimate. Underground tokens have the same functionality in their respective institutional reality, but are not recognized as legitimate by governments.
[6] Because of its physical properties gold is considered valuable and it is therefore easy to attach – to gold – the function of money.

Fiat money: Not attached to gold. They are just certificates that have resulted from a collective intentionality, and that has ascribed to them the agentive function of '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 (see Figure 2.1). 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*[7] *money*, or money that functions as such because some institutions (like Central Banks) have been given a status for expressing a collective intentionality, and can therefore impose – to a particular currency – an agentive function that is subsequently 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).

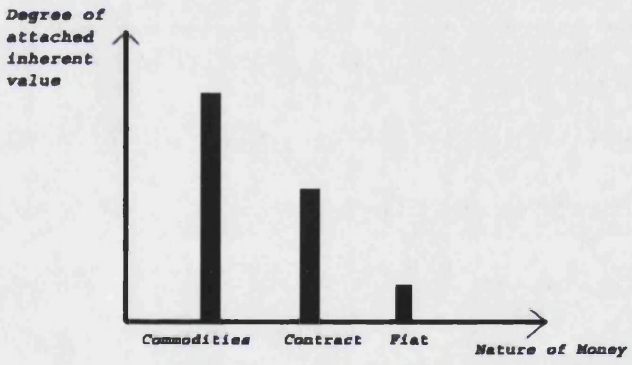


Figure 2.1: towards fiat money

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. Electronic money, which will have no reference to dollars, 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). Barriers towards that direction include: the

[7] In Latin, the noun 'fiat' means 'let it be done'

pre-established base of government issuers that will be hard to compete against[8]; that different e-money issuers will not be easily identifiable; the place of government in regulating these new monies. This transition will hard because the control-oriented and will-to-power-driven governments will not easily let go. Electronic money will create 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 (i.e. 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. 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, standardised and commonly shared agentive functions of money while the criminal origins of the entity incorporating these functions (*money*) are hidden.

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. Even though it is difficult to perceive such a differentiation, the first examples are already here and considerably test our understanding of how money functions, how it is to be regulated, or how can it open new avenues for money-laundering. Online games for example, which have introduced virtual online economies with fictional currencies, have broadened the scope of the interactivity between real and virtual cash.

[8] This has its basis on 'network economics'

In only one such game-example entitled 'Project Entropia'[9], more than half-a-million participants interact online. This virtual game platform belongs to a broader category of games categorised as MMORPGs (Massive Multiplayer Online Role Playing Games) and profits from a turnover of more than 1.5Billion 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 10PEDs are worth $1). One can transfer money into the virtual space, make virtual investments, potentially engage in fraudulent activities online, and even claim more than one identity (virtual!) for potentially laundering money through that route. In convenience, the company behind this has introduced a real ATM card (pictured below), from which the holder can withdraw money from any regular ATM. Meanwhile the money actually resides in the virtual space, and the conversion is done automatically through the virtual exchange rate. Of course a series of issues arise here, when virtual games act as financial institutions and provide banking facilities (e.g. 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 $1.5million are changing hands every day in a virtual world where the government of Sweden recently decided to open a virtual Embassy! (Spiegel 2007)

Figure 2.2: A real ATM card for withdrawing virtual money

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

[9] http://www.entropiauniverse.com

constructs of criminality, or else 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 dissertation to delve into such an issue, its 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. A clear example is in the application of *Directive 91/308/EEC* in different member states of the EU. As the 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 virtually, 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?

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 another criminal activity (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[10] (Tanzi 1996).

The laundering *process*

A fundamental distinction that has to be made while attempting to define money-laundering 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.

[10] Small sums of criminal money can be easily laundered, especially if they are below the suspicious transaction reporting threshold that banks use. This is typically in the range of $10,000.

Another way of defining ML is by portraying it as a *process*. The consensus surrounding such a definition is somewhat better, and ML is portrayed through the typical three-stage model:

i) The *Placement* Stage where the proceeds from the criminal activity enter the financial system.
ii) 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.
iii) 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[11] has altered even these, 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 the criminal to go through the placement stage, hitherto the stage where he was 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). That, along with the fact that Money Laundering on the Internet has cut out one of the two methods for detection (suspicious transaction reporting through face-to-face interaction – with the other method being monitoring transactions that exceed a certain threshold), it is no wonder that cyber-laundering has created a 'market' of around $50 billion per year[12]. Money launderers have therefore recently moved into Internet gambling, online casinos, and credit card e-transactions. The potential for illegally utilizing these new possibilities has increased considerably (Hugel and Kelly 2002).

[11] Nothing more than the application of ML in the information age, by the use of 'tools' like the Internet, mobile technologies, etc...
[12] According to a 2001 estimation from the paper of Steven Philippsohn

Section II: The myths of ML estimation

Estimating the money laundering market

One of the most difficult tasks of analysis is the estimation of the money laundering market. There have been several attempts, but before we proceed in describing the proxies that have been used for estimation, it is useful first to acknowledge once again that what constitutes ML is constantly changing. 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.

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 2-5% of the world's Gross Domestic Product, something that brings the estimate up to $600billion ~ $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 the total global ML to around $2.85 trillion (Walker 1998)[13]. If we include cyber-laundering[14], then we can add an additional $50 billion to the total estimates (Philippsohn 2001).

[13] That being the case, the author wonders why the suspicious transaction reports count for only a tiny fragment of the total volume of ML. Moreover, another issue that is posed is not the amount of dirty money at a national level but the relevant proportions of clean versus dirty money being transmitted through the financial centres, something that is particularly higher offshore.

[14] Cyber Laundering is nothing more than ML via the Internet. The problem with cyber-laundering is that the detection of the launderers is rendered even more difficult because they have the capability of complicating the money trail through various electronic transactions worldwide.

The deviations in the estimates of the ML market become more evident when we look at how many different methodologies exist for this purpose. Furthermore, and as we have previously discussed, the dynamics of the definition of ML evident from the evolution of legislation[15i], clearly poses another serious problem in estimation. The issue of defining the underground economy is still 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[ii], where estimates range from 1.4% to 47.1% 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 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 1998)

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. 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). It is therefore time to stop seeing money laundering and anti-money-laundering as separate entities that are in conflict. They are structurally coupled, and formulate an industry that is beyond good and evil[iii].

[15] This will be further analyzed in the following section

It is therefore a fallacy to consider any estimations of the underground economy as real. Rather they are only indicative of scale. 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.

► ML in the information age: it might as well be termed cyber-laundering, but it is money-laundering nevertheless. Cyber-Laundering (CL hereinafter), concerns the passage of ML into the cyber-domain 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). One such example comes from China where two hackers were given the death penalty for hacking into a bank remotely, stealing ¥720,000, and then trying to transfer the money to sixteen accounts they had created[iv] (HKVoD 1998). 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 the 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[v] 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 in 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 middle-men 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 Economic Aspect of Globalization: The second element that could be considered as a reason for suggesting an increase in the ML-market. According to a research report from the IMF, there is a clear sign that countries to have welcomed the *economic dimension of globalization* by liberalising 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 was 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. 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 participate in the new global economy. This will subsequently result in a continuously increasing capital flow, which in its 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 there is of such astronomical magnitude that with a little caution, miscreants won't attract much attention.

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.

Section III: Legislation on ML

The International Fight against ML

There have been several initiatives targeting the problem of ML, but it is beyond the scope of this dissertation to analyse fully each and every one. Furthermore, an in-depth examination of the documents 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 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 Anti-Money-Laundering domain (AML).

The major initiatives regarding AML are presented below in chronological order (where specific dates could be retrieved for the initiatives, they are presented):

1) **27 June 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".
2) **December 1988** – The Basel Committee on Banking Supervision – "Statement on Prevention of Criminal Use of the Banking System for the Purpose of Money-Laundering".
3) **19 December 1988** – United Nations – "United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances[16]".
4) **June 1990** – The Caribbean Financial Action Task Force (CFATF) – The 19 Aruba Recommendations.

[16] One of the most important international initiatives and also termed as *The Vienna Convention*

5) **8 November 1990** – Council of Europe Convention on laundering, tracing, seizure and confiscation of proceeds of crime (The Strasbourg Convention).
6) **1991** – The European Economic Commission – "Council Directive on Prevention of the use of the financial system for the purpose of money-laundering" *Directive 91/308/EEC.*
7) **5-6 November 1992** – The Kingston Declaration on Money-Laundering.
8) **18-20 June 1994** – "International Conference on Preventing and Controlling Money-Laundering and the use of the proceeds of Crime: A global approach".
9) **21-23 November 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.*
10) **1996** – Financial Action Task Force – "The Forty Recommendations".
11) **14 November 1996** – "The Riga Declaration on the fight against money-laundering".
12) **10 June 1998** – United Nations – "United Nations on attacking the profits of crime: Drugs, money and laundering". A panel Discussion at the Twentieth Special Session of the General Assembly.
13) **1999** – United Nations – "International Convention for the Suppression of the financing of Terrorism".
14) **30-31 March 2000** – United Nations – "The United Nations Offshore Forum" *Cayman Islands.*
15) **15 November 2000** – United Nations – "The United Nations Convention Against Transnational Organized Crime".
16) **October 2001** – The Basel Committee on Banking Supervision – "Customer Due Diligence for Banks".
17) **31 October 2001** – FATF – "The Financial Action Task Force Special Recommendations on Terrorist Financing".
18) **4 December 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".
19) **20 June 2003** – FATF – "The Forty Recommendations" *Revised.*

20) **26 October 2005** – European Commission – '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, including terrorist financing' 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 Anti-Money-Laundering 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 has been attempts from the early 80s to address the problem (e.g. 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*, and it is this term that will be used henceforth in this dissertation.

► **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[17] trafficking crimes (thus money-laundering didn't 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[vi]. 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) – *Article 3.*

[17] Not surprising for a first attempt to tackle the problem internationally, as drug trafficking produces large sums of money that need laundering. Targeting the proceeds of crime also targets crime itself.

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*[vii], *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. Further, 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 (Drug Control Programme) added an additional step, providing help in legislation and drafting a *Model Law in ML*, in 1993. Law enforcement agencies, which played a major role in that initiative, included the ICPO/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% of the messages being exchanged through that system are drug-related and of immediate interest for the fight against money-laundering (Gilmore 1999).

► The **Financial Action Task Force** 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:

a) The Forty Recommendations in 1990.

b) The *Revised Forty Recommendations* in 2003.

c) Eight special recommendations on Terrorist Financing in 2001.

Even though the FATF cannot pass laws, it only makes recommendations, however, these are received with widespread trust and so the FATF has been recognized as the major contributor in the global 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 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[18]. 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 established by the heads of State or Government of the seven major industrialized countries and the President of the European Commission **remained the standard** by which the measures against money-laundering adopted by concerned States should be judged ..." (UN 1998) – *emphasis added.*

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 termed as 'black-listing'. Typically, the countries that do not have sound AML policies are those that are black-listed. 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 has not promptly dismantled the legal and banking havens of the Crown Dependencies remains unsettled. One might say that political will is inversely related to the amount of money surrounding the country. The fact remains that this connection between the UK and its protectorates has crowned

[18] Commission on Narcotic Drugs resolution 5 (XXXIX) of 24 April 1996.

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 work within the same systems. 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 the MI6, and was desperately trying to keep his role secret (Rider 2003).

Nauru[19] may be a country that is a long way away from the Paris-based FATF, but it is still under considerable pressure from the threat of financial countermeasures (Johnson 2003; Roule and Salak 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 evolution of FATF's working agenda speaks for itself.

The reality is that the FATF has expanded, and it has become extremely powerful. 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 black-listed initially responded negatively, but soon recognized that improving their procedures would get them

[19] With a total land area of 21 sq km, Nauru is the smallest republic in the world. But in ML, even the smallest republic can 'contribute' significantly.

accepted. Subsequently the vast majority wholeheartedly joined in with the international AML effort (Johnson 2001).

However, after the terrorist attacks on US soil on September 11 2001, 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. Firstly, terrorist activities are often funded by legal money. Secondly, 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. Thirdly, 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. Banks are being forced into policing legitimate transactions that could potentially be used for terrorist purposes (ibid). Furthermore, it is evident that the hopeful pre-emptive strike against ML and terrorist financing may cause more problems than it actually solves. 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** 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 1998).

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[20]:

> "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 1998).

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 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[21]**. 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.

---

[20] 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".

[21] 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 I of the aforementioned resolution, the United Nations Convention against Transnational Organized Crime entered into force on 29 September 2003.

Article 6, the 'Criminalisation of the laundering of proceeds of crime', mentions 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 route through the banking institutions. According to Article 7:

> "Each State Party 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." *Article 7 (UN 2000)* – emphasis added.

► The Basel Committee on Banking Supervision Initiatives.

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 '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[viii] (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 United Nations and the FATF. The focus of Basel's work in respect of terrorist financing was to improve Know Your Customer and Customer Due Diligence standards *for all categories of institutions that provided financial services* (Basel 2002).

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 analyzed. These are: *Mutual Legal Assistance (MLAT),* communication between Financial Intelligence Units (FIU), which are based on *Memoranda of Understanding (MOU)*, and supervisory channels[ix].

As communication received special attention in this paper of the Basel Committee, there was also an identification of several areas of future work. These would be 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 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 2003)

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[22]. 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 analyzed 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, on-going 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 2003).

[22] Such structures are can often be found in offshore centres.

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 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[23]'. 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.

Directive 91/308/EEC was complementary to the aforementioned initiatives in the EU and was influenced by the Forty Recommendations. 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)[x].

[23] That was the very first focus on ML from an international organization

Directive 2001/97/EC amended the directive of 1991. Here, EU legislation is extended to cover all organised 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

There is no doubt that the major shift of emphasis in the latest proposed Directive of the European Commission (also known as the 3rd Directive) involves what is termed the risk-based approach. Dominance of the term 'risk-based approach', which includes a tremendous number of ambiguities, will be analysed in the final chapter of this dissertation after both the theoretical treatise on Systems Theory is presented and the findings from the research outlined.

What follows is a table summarizing the major initiatives and their contributions.

Table showing the major contributions of the international initiatives (*Table 2.1*)

Year	*Name of Initiative*	*Major contribution*[24]
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.

[24] No value-judgment is being made by the use of the word contribution. Some initiatives may have had or may have results adverse to those they try to achieve. Terrorist Financing is a potential candidate.

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 - *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.
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 - *Proposed Directive COM(2004)448*	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 (e.g. as in the case of high-risk customers)

Table 2a: Summary of major legislative initiatives

Section IV: Chapter Epilogue – Overview

An overview of some 'global' AML features

It is useful here, 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 the flavour of ML and the networks that operate globally. Perhaps more importantly, they invoke the challenges that the AML community is facing. The purpose of this section is not to draw a map of the ML network, as this can only be done in approximation, but to provide the reader with a sense of what the global ML and AML community looks like.

Figure 2.3: A(ML?) networks

In Figure 2.3 above, there are three types of connections. The blue dots represent those jurisdictions that have been – at some point – featured in the famous FATF black-list. The red dots represent countries that are not IMF members, and finally, the yellow ones represent the G7.

Let us start by the non-surprising 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).

What is so special then about black-listed countries? The Financial Action Task Force would probably respond by saying that the jurisdictions that are black-listed 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 for 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 bio-chemical equipment (via the Internet) that ended up mostly in the middle-east, all through a shell company and on a discount reaching 80% of the purchased price (Demetis 2004)[xi]?

Such inconsistencies become more evident in particular examples within the AML community. Nauru, the smallest republic in the world, has refused cooperation after being black-listed, and has also managed to launder around $70 billion in 1998 (Lilley 2000). Nauru demonstrated to the world that geographical isolation[25] has nothing to do with ML, especially when it is supported by a full Commonwealth membership[26]. Black-listing from the FATF would soon follow (with a 2 year lag!) and even though it is generally perceived that black-listing causes trouble for business (as countries face barriers whilst transacting with the world's largest economies and other AML community members), it seems that there are several jurisdictions that don't mind black-listing. Because of the nature of the money-laundering phenomenon, money can be channelled and laundered in various ways.

Nauru was placed on the FATF black-list in 2000, and in 2001 passed its AML Act. With a change of government in Nauru, 139 offshore banking licences were revoked

[25] Closest neighbour to the island is Ocean Island, located 305 Km to the East.
[26] There are of course quite a few Commonwealth members that have been on the FATF black-list like Barbados, Tuvalu, etc.

(Johnson 2003). However the AML Act failed to meet the obligations (according to the FATF) and then the OECD declared probable sanctions against Nauru, something that was followed by 18 countries requiring increased scrutiny in all transactions involving Nauru (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).

The example of Nauru provides a good opportunity for discussing several issues. First of all, even if Nauru's AML Act met the obligations, it would be highly unlikely that ML would cease to exist. Changes in legislation that target ML are always welcome (by the FATF), but even if they are in place, they may be introduced just for the sake of complying with the international community. If we consider the number of countries that requested increased scrutiny in transactions involving Nauru and put this number in a global perspective (18 countries out of 193), then that did not even come close to the membership size of the FATF, let alone the international community. It therefore becomes evident that even if black-listed, Nauru 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 current black-list[27]. Furthermore, in their effort to impose sanctions to 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 remains to be seen, but such sanctions imply that international cooperation on AML has reached a high level of information sharing that even indirect transactions can be monitored.

This is, however, far from reality. There are 191 members of the United Nations, 184 members of the International Monetary Fund, and 100 members[28] of the Egmont Group (thus only 100 countries have recognised Financial Intelligence Units). This poses a serious problem as the sharing of information is limited between countries that have an

[27] FATF decides to impose counter-measures on Nauru on December 5, 2001. The country is still black-listed (as of July 12, 2004)
[28] 16 of which joined the Egmont Group in 2003.

FIU and those that don't. Things became even more problematic as there are no formal mechanisms to request information from countries that do not have an FIU, thus coordination is gravely jeopardised. As for the Financial Action Task Force, it numbers 33 members, and does not wish to expand its membership. There are of course other FATF style groups, like the Caribbean FATF, and other organizations, like the Basel Committee, the World Bank, the IMF, etc that target ML. Far from providing help, organizational opportunism on a domain like AML can dramatically increase the complexity and render coordination and cooperation dysfunctional.

This may considerably put into question the very function of organisations like the FATF. Severe criticism has been levelled at how the FATF deals with countries that become black-listed, 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?* "[29]

One might perhaps offer a series of criticisms in these assertions, including the impossibility of effectively scrutinising and reviewing every country globally, 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 – unavoidable perhaps – 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

[29] Taken from http://www.dirtydealing.net , Peter Lilley, 2006 – *emphasis added*

should be considered more 'risky' in ML and 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 dissertation in April, 2007 – *no countries* whatsoever are currently being featured in FATF's infamous list. 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 TF, 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 and 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), and economic aspects beyond financial issues that are also deemed to be of importance.

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 World Bank. Interestingly enough, 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 black-listing until a consensus was reached (Holder 2003). Of course, and despite considerable IMF efforts for expansion to the AML domain, the FATF black-listing 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 UN counts 193 countries on the globe. As previously mentioned, there are 191 countries that are members to the UN. The only two territories recognized as countries that are not members of the UN are The Vatican City and Taiwan. Both have been heavily involved in money-laundering, but the Holy City provides a magnificent example. When the Vatican got its opportunity to be recognised as a sovereign state, capital flight was strongly encouraged, Mafia money washed through, and there were opportunities aplenty. The Vatican invested in gold, Swiss holdings, etc, and it is estimated that the Vatican's investments around the world are worth an approximate

$15billion, making it the single most important owner of equities (Naylor 1994). One of the sources of the invested money has potentially come from the Nazi Croatian Treasury that was illicitly transferred to the Vatican Bank[xii] - via banks in the United States (ibid). Such are some of the complexities and ironies of the (A)ML community.

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 forty recommendations. This clearly demonstrates that despite the clear progress that has been made throughout the last 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 also has 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 dissertation is claiming, it is that of dealing with AML through Systems Theory. It aims at providing truly systemic considerations and insights that surpass by far the purely experimental and descriptive levels that seem to have exhausted their possibilities, and rarely go beyond a mere pragmatic-typological based treatise.

Chapter III: Research Methodology

Chapter Structure

This chapter is structured as follows: first, some introductory comments are offered regarding methodology that attempt to clarify the foundational circumstances under which any research methodology should be based. Following such an introduction and subsequent analysis, a broader framework for methodology is developed that covers all the stages of the research process. This is separated into three distinct stages: Stage 1 involves the determination of the philosophical presuppositions that guide any research, Stage 2 determines the research design and collection of data techniques, and finally, Stage 3 reflects on the way that data can be coded, a theoretical framework applied, and conclusions reached. The synthesis of these three stages constitutes the broader structure for methodology that is applied in this dissertation. Following the presentation of such a broader methodology, each individual stage is then applied for the purposes of the specific techniques used in this dissertation, so that the reader gains an insight into the clear methodological path that has been chosen.

Introduction

Having taught the subject of research methodology for three consecutive years to the Masters students of the Information Systems Group at the London School of Economics, I feel indebted to start the exploration behind this chapter by thanking all of my students. With their persistence and insightful questions on what constitutes legitimate research, they have provided me with many reflections on methodology. These reflections have considerably expanded my own understanding of the critical issue of methodology, and for that I am sincerely grateful to them. They have helped me

greatly in elevating methodological issues that are considered by many to be a somewhat boring – yet necessary – subject-matter, to one of the most interesting aspects for consideration in research.

Before engaging in the task of differentiating between the different theoretical perspectives, and clarifying what is the research methodology behind this dissertation (in its scope, philosophical underpinnings, data collection and analysis methods), it would be prudent to acknowledge that any research stems from certain epistemological and ontological positions. These positions are predominantly philosophical, and hence must be treated as a matter of belief – a starting viewpoint on how the world can be described, and ultimately, how research can commence. Following this assertion, all legitimacy and rigour that the author of a research dissertation tries to claim can only be criticized on the grounds of its consistency to the predominant methods of the paradigm to which he subscribes. Displaying this consistency is perhaps the most crucial issue, and one has to delve into the criticisms of his own research approach only to confront them constructively and innovatively.

In the first part of this chapter I will delineate between four widely discussed categories that are encompassed in the framework of Burrell & Morgan. These categories are often utilized in research in information systems, and have become one of the many – yet predominant – classifications and schemas upon which worldviews are expressed (Klein and Hirschheim 1987; Angell and Smithson 1991).

After a brief examination of each of the paradigms, I will attempt to provide a clear account of what the underlying methodological foundations of this research are, and subsequently position this dissertation using the paradigm that is more appropriate in this context. This methodological overview will be carried out by utilizing a range of resources, and aims at providing a high-level theoretical conceptual map of methodology; this higher-level structure will be applied for the purposes of this dissertation so that the choice of steps throughout the methodological structure become evident.

According to Burrell and Morgan there are four basic paradigms: The Functionalists, the Interpretivists, the Radical Structuralists and the Radical Humanists (Burrell and

Morgan 1979). As outlined in Table 3a below, these are separated into two basic dimensions. The first dimension refers to epistemological beliefs, and the second dimension delineates between the sociology of regulation and the sociology of radical change.

	Objective	Subjective
regulation	FUNCTIONALIST	INTERPRETIVIST
radical change	RADICAL STRUCTURALIST	RADICAL HUMANIST

Table 3a: The Matrix of Burrell & Morgan

In order to avoid confusion, there first has to be a clear account of what constitutes a paradigm as the categories within the B&M matrix are usually referred to as paradigms. Much of the conceptual constructs for defining the idea that we have come to term as 'paradigm', source from the pioneering work of Thomas Kuhn in his 'Structure of Scientific Revolutions'. For the purposes of the analysis that follows, a paradigm is considered to be a unitary package of beliefs about science and scientific knowledge (Kuhn 1970). Even though there is always some ambiguity about what constitutes a paradigm, the ontology of the paradigm (its very existence) serves a specific purpose; that is, to set boundaries so that research can proceed whilst the 'unnecessary' complexity is cut down. Reduction of world-complexity therefore becomes an ontological presupposition for the construction and utilization of a paradigm. Behind this assertion lies a fundamental reasoning that delimits our viewpoint on the research process. It is this delimitation that allows research to proceed. But at the same time such delimitation renders the application of theories imperfect. This is precisely why 'theory is both a way of seeing and not seeing' (Walsham 1993). A specific theory may be 'working' correctly under certain assumptions, but it may be completely incompatible at a different context. Thus, complexity is cut down through paradigm delimitation, an act of choice that restricts the examination of a research area.

It comes as no surprise then that Burrell & Morgan (B&M hereinafter) assert that the four outlined paradigms should be considered as mutually incompatible. Of course, the problem is that category is not truth, but merely cognitive fiction, an act of choice (Angell 2000).

Methodology

The etymological foundation of the word 'Methodology' comes from the combination of two Greek words: 'method'[30] and 'logos'[31], which can, once considered together, translate as 'to speak about method'. Within a scientific context, methodology implies the outline of a foundational platform upon which a particular research project can be delineated. The outline in itself highlights *the tools of scientific investigation*, and these tools are selectively chosen by researchers, all the while they constitute a body of practices, procedures and rules used by those who work in a discipline. Of course, there is no doubt that any methodology is by definition flawed, as it contains a necessary reduction of complexity, and therefore one is forced to choose from a vast multiplicity of scenarios in order to address a supposedly well-defined problem. Gödel summarised this assertion in his *incompleteness theorem,* stating that all theoretical formulations are necessarily incomplete. When one chooses a research strategy one determines both how the phenomenon being studied will be revealed, and indirectly, the consequences of the knowledge thus generated (Gödel 1986). This is of course a clear epistemological position that is being put forward by Gödel, one that I fully subscribe to for the purposes of this dissertation, and one that is fully compatible with the epistemological assumptions followed here, and elaborated in this chapter.

Method however often surpasses the Gödelian incompleteness, and when appropriated it often gives the delusion of coherence. This has been amply demonstrated by the seminal works of Paul Feyerabend, where method becomes either too restrictive or the background against which ideological battles take place fuelled by varied epistemological and ontological grounds (Feyerabend 1975; Feyerabend 1987). The

[30] Μέθοδος
[31] Λόγος

problem therefore is method itself; and such a problem is a truly foundational one that affects not only the field of Information Systems that has been through a series of identity-crises as a discipline (Avgerou 2000; Avgerou and Madon 2002), but also and equally, disciplines like mathematics that seemingly enjoy 'more coherence' in their internal structures, while social sciences appear to be degraded to a somewhat inferior set of concepts with purely descriptive capacity.

But such has been the plague of functionalism or positivism throughout society, that the fundamental problem of method has become somewhat distorted, and a belief that numerical manipulation is somehow superior to other forms of scientific investigation is now dominant. This belief has since become a transcendental property that has infected nearly all disciplines, even those that fall outside the scope of positivism and are methodologically based on a different set of tools for scientific investigation. Since this is an ongoing debate within the field of Information Systems, and one that has lasted many years (Lee 1999), I feel I have to address this methodological (and mostly epistemological) issue from a basic standpoint and through a simple example by providing a few reflections.

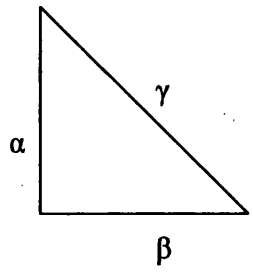
What is the need or the driving force behind all these operations, which leads them to acquire a mathematical description? Why should an observation acquire functional (i.e. mathematical) notations, and succumb to positivism? Are there any alternatives? Did this problem always pose itself like that?

The answer to the latter question is no; the problem has manifested itself in many different ways, and has fabricated and replicated itself in a self-referential manner throughout all scientific disciplines. **There is nothing** inherently mathematical in either the physical or the social world; and nothing inherently mathematical (and even worse linear) in observation, which is the means by which we acquire knowledge. *It has to be made clear that mathematics (the main pillar of positivism) is merely one notational schema amongst others, and that there is simply* ***no way that any notational schema can describe itself without reference to another notational schema (e.g language).*** Mathematics can certainly develop self-referentially (i.e. theoretical mathematics), but the moment it seeks to describe something (or be described), it has to attach itself, or allow itself to be attached, to another notational schema. Systemically, this constitutes

notational interpenetration, as nothing can exist in splendid isolation, not even notational schemas. They too are nodes in a network with no focal point whereby, in the simplest of all scenarios, they refer to an external reality that they are seeking to describe.

There was a point in time that this problem was exposed to a different degree of granularity than now; an example comes from the school of Pythagoras, and the famous example of the Pythagorean Theorem. The degree of the problem was ameliorated by the fact that Pythagoras and his school tried to *provide combinations of notational schemas despite the geometric/mathematical* treatise of their subjects, as they also sought to provide a qualitative explanation for the quantitative results; that was a requirement essentially deriving from the projected *philosophical and qualitative rationality* that was imposed on numbers. Anything 'irrational' was an abomination.

The Pythagorean Theorem



$$\alpha^2 + \beta^2 = \gamma^2$$

Figure 3.1: The Pythagorean Theorem

Rumour has it that when an abomination was uncovered by Hippasus, a disciple of Pythagoras, a few Pythagorean students drowned him at sea[32]. Apparently, Pythagoreans were very sensitive towards 'rationality', whereby everything could be expressed through integers or as ratios of integers; in that way, they could interpret it in

[32] Heath, pp. 65, 154, vol. 1, as cited by Stillwell.

the qualitative sense. But when Hippasus applied the Theorem to the scenario whereby both α and β equalled to 1, he came up with something that looked like $\gamma^2=2$. The conclusion followed that γ equalled the square root of the number two (of course the concept of the square root had to be constructed before this previous statement may even be made); an entity that was not only irrational but also infinite in its mathematical expression, the first thirty digits of which could be estimated as follows: 1.41421356237309504880168872421.... Multiply that number by itself **(another self-reference[33]! Whereby the operation forces the number to refer to itself)** and you would approximately get the number two. One of the first schisms between quantitative and qualitative descriptions had forcefully presented itself, and left the Pythagoreans wondering at the paradoxical implications. *How could it be that a side of a triangle (the hypotenuse), which can qualitatively be described as a fixed length, have a quantitative expression that is denoted by a number that is represented by an infinite sequence of non-zero digits, particularly when that number emerges from two simple 'rational' numbers?*

The point made by using this example is simple: for any scientific discipline, asymmetry becomes a foundational platform for the self-reference of the discipline itself, and its evolution. Without asymmetry, knowledge becomes impossible as it collapses into tautological structures. With asymmetry, knowledge becomes possible as variability in choosing the generation of knowledge becomes equally possible: such is the endeavour we call method.

How the Information Systems field has ended up being generally underpinned by a positivist epistemology is therefore an issue of convention, power, and paradox. For what can be made of the fact that more legitimacy is perceived in studies that utilize hypothesis-testing by attributing numerical values to highly interconnected parameters than by taking extremely contextual issues into account, leaving them suffocating in the background?

This attack on positivism is not intended to isolate it conceptually as an illegitimate form of research; however, it does attempt to demonstrate that validity is based upon

[33] What is described here as self-referential is in a sense all the higher-powers of numbers as the result of a multiplication of a number with itself, again, and again, and again ...

epistemological assumptions that cannot – and must not – be taken as universal truths, or seen as the one and only way for undertaking research. This of course does not exclude the possibility of using the outcomes of positivist-based research within the context of interpretivism, and as this is the case with this dissertation, an attempt to make such a structure more explicit is made here by providing the methodological outline.

A broader structure for methodology

In what follows, a broader structure is provided that penetrates all aspects of methodology, from the very beginning, right up to the very end of the research process. This high-level structure will be applied to this dissertation so that the research methodology – and ultimately the 'reduced-in-complexity' path that has been chosen – becomes clear. Part of the conceptualization behind this structure is based on the Burrell and Morgan framework (Burrell and Morgan 1979), on John Dewey's analysis of the *double movement of reflection* that will be utilized at the very end of this structure (Dewey 1933), on various other resources that critically examine methodological issues (Yin 1984; Chua 1986; Kaplan and Duchon 1988; Orlikowski and Baroudi 1991; Searle 1995; Myers 1997; Baskerville 1999), and finally on personal methodological reflections that were derived from teaching the subject matter for a period of three years.

Figure 3.2 below attempts to synthesize the broader methodological structure on the basis of the resources referenced above and to delineate the process into three distinct stages.

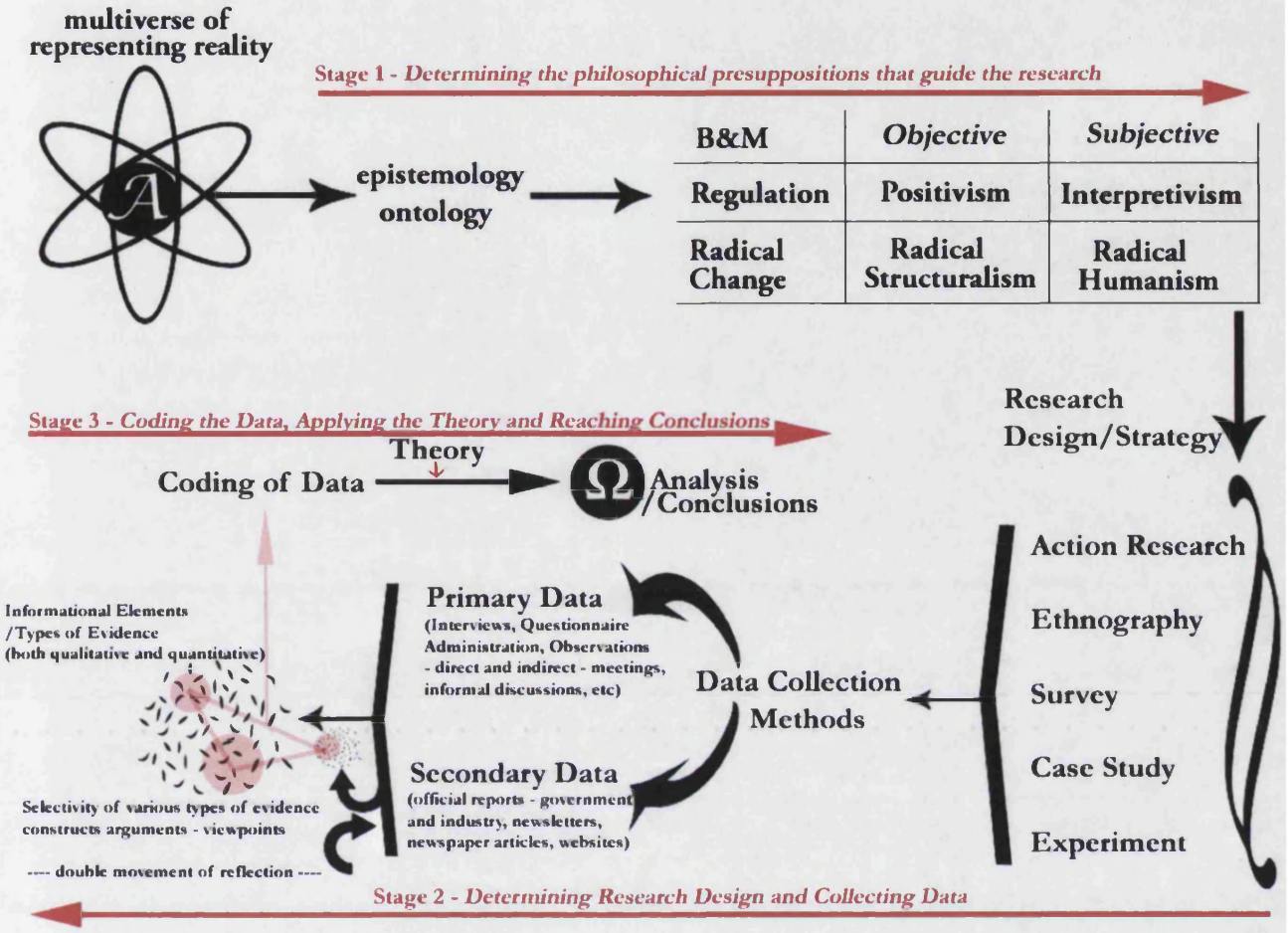


Figure 3.2: A broader structure for methodology

In the first stage of the methodological outline, the philosophical presuppositions that guide the research process must be determined. In the second, reflections are necessary for determining the research design and the process of data collection. Finally, in the third stage of methodology, data-coding and selectivity of various types of evidence needs to be justified; in this latter stage, the applying of theory and the reaching of conclusions takes the form of a 'double movement' of reflection (see Dewey below). These stages are described in turn in order to provide the broader coherent methodological structure upon which this dissertation rests.

Stage 1: Determining the philosophical presuppositions that guide the research

The starting point for any research orientation in any discipline constitutes the realization that there is a vast array of possibilities in representing reality (and perceptions about reality). The quest therefore for any research project starts from fundamental epistemological and ontological positions. Ontology relates to perceptions about reality or 'Being' in the world. Philosophical treatises, such as that of Searle on '*Does the real world exist*' (Searle 1995), deal with primary ontological positions. Mundane as such questions may appear to some, they do play a critical role, knowingly or unknowingly, in how research is directed towards epistemological matters (how we know what we know). If for instance one believes that the 'world' exists independently of any human interference (e.g. cognition) and that 'Being' is real and external, one would believe that there is an objective reality (a reality 'out there') that is independent of any observation, and one could attempt to extract the laws of that reality accordingly. In such a scenario, one possibility is to assume cause-and-effect relationships within that objective reality, and to attempt to extract these by deduction. This outlook is referred to as the philosophical standpoint of *positivism* (functionalism and positivism are used interchangeably here in the context of the Burrell and Morgan matrix – B&M hereinafter).

The identified variations of philosophical standpoints are so many in number that a review of all would require volumes of dissertations (in pure philosophy alone!). As this dissertation does not share that goal, it attempts instead to provide a few comments to demonstrate the complexity behind isolating different epistemological perspectives before collapsing them into the simplified form of the B&M matrix. Positivism for example (it owes its name in the belief that knowledge is firmly grounded in something that is *posited – or given*) claims to grasp objective meaning, however, even in doing so, researchers are able to differentiate between twelve (!) or more variations of positivism (Crotty 1998). As Crotty remarks on positivism:

> "If we were to say that the world of a positivist is a 'mathematical' world we would probably be in! A world which is quantifiable. However, the scientific world is an abstraction from the world we live. The world perceived through the scientific grid is highly systematic and organized, full of regularities,

> constancies, uniformities. It is in high contrast with the ambiguous and uncertain world we experience every day... Arguing with positivism must not be done with what positivism does but *to the status it ascribes to scientific findings.* However, at the 20th century, more scientists have challenged the claims about objectivity leading to a less arrogant form of positivism. Probability is in, certainty is out. No absolute objectivity but a certain level of objectivity. *This is known as 'post-positivism'"* (ibid).

From the Vienna Circle to Kant and Comte, positivism has gone through a series of mutations, while even Physics with the advances of Heisenberg and Bohr in Quantum Theory have sent shockwaves of uncertainty through it with the famous *uncertainty principle*. In creating disbelief in absolute objectivity, the two helped create a post-positivist philosophical standpoint in the most unlikely of all disciplines: Physics itself. The impact of such an evolution is not to be taken lightly, for it has profoundly shaken the foundations of positivism.

It is clear that the multitude of epistemological consequences of so many variations has given way to a multitude of representational schemas that attempt to classify, simplify and collapse the complexity of the underlying problem domain. The B&M matrix is used here as a simple classification schema, as it has been broadly used within information systems research (Angell and Smithson 1991) (Klein and Hirschheim 1987). In the B&M matrix the two basic dimensions refer to epistemological beliefs (objective and subjective), and to perceptions of social reality (sociology of regulation and sociology of radical change). Positivism (or functionalism) in the context of B&M represents the belief that society is governed by laws of causality, and that it can be studied just as Physics studies nature. To positivists, even uncertainty can be causally dissected.

Instead of an objective world that is posited, the advocates of Interpretivism see a shared social reality. They break the strong link between cause and effect, and adopt a nondeterministic view of the world. They believe that people create their own subjective and inter-subjective meanings as they interact with the world. Deterministic assertions are hard to make because reality is seen as social construction and interpretation by actors who are trying to engage with their understanding.

A commonly held misconception, that *interpretivists use only qualitative methods* since such methods offer interpretation of the examined phenomena, will be resolved here. Indeed, in Chapter V where the narrative of the case study is outlined, the reader will observe that quantitative methods are often used in order to corroborate data that has been collected from interviews. In doing so, this dissertation submits to a combination of data types that are both quantitative and qualitative. That however must not be taken as an underlying epistemological ambiguity; quite the contrary. There is nothing contradictory in utilising both quantitative and qualitative data within the scope of a particular research design that is informed by a specific epistemological stance. Resolution of such an ambiguity, often the target of many researchers (Miles 1979), can be achieved only when differentiating between two distinct aspects of the research process; that is, differentiating between a research design (also known as a research strategy) and data collection methods (Yin 1981; Yin 1984). In this manner, it needs to be made clear that one is able to choose a particular research design (such as a case study) that is informed by certain epistemological beliefs, and subsequently proceed into data collection methods that can be both quantitative and qualitative. This then becomes a matter of emphasis, and determines whether qualitative data become the primary focus, data that are subsequently corroborated with quantitative data or vice-versa.

Stage 2: Determining Research Design and Collecting Data

Following on from particular philosophical presuppositions that guide the research and constitute a particular epistemological and ontological position, one subsequently decides upon a particular research design or research strategy. Examples of such research designs are portrayed in Figure 3.2, such as action research, survey, case study, etc. Following the decision of a research strategy, one moves on to data collection so that *primary data* can be differentiated from *secondary data.*

Primary data collection methods can be interviews (unstructured, semi-structured, or structured), questionnaire administration, observations that can be either direct or

indirect, meetings, informal discussions, etc. These can be supplemented by secondary data, such as government or industry reports, newsletters, newspaper articles, website material, etc. The totality of both primary and secondary data gives rise to a collection of disparate data that can be both quantitative and qualitative. In Figure 3.2 that depicts the evolution of the entire methodological approach, these are portrayed as 'informational elements' whereby the types of evidence are classified into two distinct categories (quantitative and qualitative).

As the data collection process commences and continues, it becomes clear that selectivity of various types of evidence (whether qualitative or quantitative) gives rise to arguments and viewpoints in respect of the research being undertaken. Arguments are constructed on the basis of the data collected, but soon enough the entire process repeats itself as arguments will often require corroboration, further insights, and more in-depth data collection (i.e. additional interviews on specific topics). These in their own turn generate yet more data, and the process continues until the researcher is satisfied with the corroboration of several subjectively – in their scale of importance – identified streams of arguments. This oscillatory process between data already collected that are used to begin the construction of arguments, and the collection of yet more data that corroborate the arguments already selected for a more in-depth analysis and in doing so generate more data that could proven irrelevant for the purposes of the researcher, is what John Dewey terms as the double movement of reflection (Dewey 1933). Selectivity of data following the completion of this process leads on to the final stage of the research process.

In that process, it is very important to note that the combination between quantitative data and qualitative data is not only possible, but also contains no epistemological paradoxes. The close coupling between quantitative data with research identified as positivist is merely a convention that does not prevent incorporation of quantitative data within interpretivist research.

Stage 3: Coding the Data, Applying the Theory and Reaching Conclusions

Coding the data then implies that specific streams of evidence are put together for the presentation of particular arguments. This is typically done when the research findings are being presented (in this dissertation this refers to Chapter V). Prior to the presentation of the research findings, the theoretical framework is presented (Chapter IV here). Finally this culminates in both the broader analysis of the research findings – with the help of the theory – and the provision of conclusions and insights (in this final chapter).

In applying the general structure for methodology outlined above to this dissertation, the following considerations are presented:

Applying Stage 1: Determining the philosophical presuppositions that guide the research

a. On Epistemology

This research is informed by the epistemology of subjectivism. Subjectivism (as opposed to objectivism) maintains that there can be no objective *meaning* in the object of study. Those informed by an objective epistemology claim that things exist as meaningful entities independently of consciousness and experience, in a fashion that objects have truth and meaning residing in them (Crotty 1998). As this research is informed by a subjectivist epistemology, it is believed that meaning is constructed and does not reside in the object of study. The idea that meaning is constructed from the interaction between the subject (i.e. researcher) and the object, in a way that reality is shared is also referred to as *constructionism*, an 'ism' that corresponds closely to interpretivism within the B&M matrix. According to Crotty,

> "Constructionism takes the view that all knowledge and therefore all meaningful reality as such, is contingent upon human practices, being constructed in and out of interaction between human beings and their world, and developed and transmitted within an essentially social context." (ibid)

The appropriateness of the foundation of a constructionist epistemology for this research becomes obvious when one considers the myriad of factors that influence the domain of Anti-Money Laundering. Firstly, the very idea of what constitutes money laundering is socially constructed and depicted in legislation, as has already been discussed in the introductory chapter. Secondly, because of the nature of the problem domain and the inherent ambiguity in several crucial factors (i.e. suspicious transactions thresholds, the very concept of suspicion, etc), even the ideals that are 'narrowed down' in legislation are open to multiple interpretations, and sensitive to multiple operational subtleties and contextual differentiations. Thirdly, as it has been analyzed in Chapter II, money-laundering unavoidably rests upon a pre-existing fabricated and socially constructed ideal, that of money.

On different grounds, the internationalization of natural sciences and their wide acceptance of objectivism (before chaos theory and uncertainty via quantum mechanics confused the issue) is the result of a *strictly formulated culture*, one that is based upon the principles of a 'rigid' mathematical construct, whereby its proponents consciously and deliberately try to ignore the social. However, such uniformity in scientific culture and theoretical constructs are impossible to uphold when there are social, economic and political factors that are perceived differently. Any imposition of an objectivistic-informed framework to map out the socio-political context would restrict the plurality and heterogeneity inherent in the social sphere. Hence, even with methodologies that are employed in AML under an objectivistic informed epistemology (e.g. for estimating the volume of the ML market), their inadequacy is quickly exposed when the problem remains that, from a semantic point of view, there is hardly any consensus on what constitutes money-laundering. This is of course intrinsically related to the issue highlighted throughout the AML domain: the difficulty in defining what it is to be regarded as suspicious. The problem is without a solution; any attempt to objectify epistemologically the domain of ML will automatically be undermined by its subjective ontological ambiguity. Money is a socially constructed ideal, and therefore its ontology

is socially set. Consensus and static definitions on socially constructed ideals are far from reality. The same goes for money-laundering, which has to rest on suspicion (recently confused even more by the even more elusive concept of risk) and the use of STRs as the mechanism that sustains this process.

b. On Ontology

Beliefs about ontology are equally important, and probably emerge with epistemologies as the two are intertwined. This research follows the ontological stance of **realism,** which suggests that there is actually a reality in existence and outside of the human mind. The only fundamental and crucial distinction that must be made at this point is between the concept of existence and that of meaning. The fact that there is an array of realities out there has nothing to do with our interaction with them; it is only the interaction that can give rise to a meaning. Adhering therefore to a realist ontological position implies nothing about how that (perceived) reality is being constructed and interpreted, and therefore the two positions adopted here, those of a subjective epistemology and a realist ontology, are theoretically compatible.

Applying Stage 2: Determining Research Design and Collecting Data

a. On Research Design

Before getting into the details of the research design, it would be useful to ponder the problem of the duality of research questions. One refers to the descriptive research type, and the other to the explanatory research. The first examines or describes *what* is going on, while the latter examines the underlying reasons or the *why*. The first presents considerable weaknesses, as descriptions[34] can be endless. However, the proponents that dismiss this type of research fail to acknowledge that a good description of a problem area can be very important for our understanding of it. Furthermore, a rigorous

[34] However, there are no absolute facts or absolute truths in systems as complex as society, only mere descriptions. A convincing description can therefore prove invaluable in shedding light on subtle problems

description is a considerable step for the passing to the explanatory stage. Without a sufficient description of what is going on, there is absolutely no point in explaining the why. In other words, if the basic premises are problematic, then proceeding in examining the underlying reasons becomes twice as problematic. Thus, additional emphasis must be given whilst trying to describe the phenomenon that is being examined.

It is equally important to take into consideration that a research design must be distinguished from the research method (research method here is equivalent to data collection methods as outlined in Figure 3.2). Choosing a research design does not imply or determine that a particular method of data collection will be adopted. Examples of research design include experiments, case studies, longitudinal designs, cross-sectional analysis, etc. Furthermore, by choosing a specific research design, one aims at reducing the complexity and ambiguity of collecting too much data, or data that do not closely match the research questions. In addition to the latter, the most important thing while developing a research design is demonstrating both internal and external validity.

Internal validity refers to the extent to which the structure of a research design helps in the drawing of 'solid' conclusions from the results. In other words, we must always strive for clarity, demonstrating why alternative descriptions from our findings might be less trustworthy and inconsistent.

External validity refers to the extent to which results from a specific study can be generalized. This is probably one of the most challenging areas while carrying out research, and it must be handled with caution. A typical threat in generalizing from the findings is the use of unrepresentative samples and issues of categorization. Producing generalizations must therefore take into consideration sampling issues, and be consistent within the 'category' of the specific case. Cross-context generalizations inherit further difficulties, and they tend to be more abstract (and sometimes less useful). At the conclusion of this dissertation, where the practical and theoretical contributions are described, the issue of generalisation for the broader AML system is considered.

This study focuses by using a *case study research design.* Case studies have in the past been perceived as constituting some inferior form of research for all the wrong epistemological reasons (Yin 1981), and mostly because of a widespread support for positivism (ibid), which was then at its peak, implying that unless equations can model the problem domain, then no serious attempt could be considered plausible. Because of such skewed epistemological positions, it took some time before case study research was considered to be a legitimate form, and studied carefully as such. Case studies are often seen as examples of *qualitative research,* and closely connected to Interpretivism (Yin 1984). The case study is a research strategy, which focuses on understanding the dynamics present within single settings. Case studies can involve either single or multiple cases, and numerous levels of analysis (Eisenhardt 1989). Case studies typically combine data collection methods such as archives, interviews, questionnaires, and observations. There can be several combinations. One is combining quantitative data from questionnaires with qualitative evidence from interviews and observations (ibid).

Due to the nature of the phenomenon being studied, and the confidentiality agreements agreed with the institution where the research was carried out, the name of the financial institution that has been studied cannot be revealed. For these reasons, the financial institution studied in this dissertation is referred to as 'Drosia Bank', details for which are analysed in Chapter V.

b. On Data Collection

A considerable volume of findings in this research are derived from interviews, the majority of which were unstructured. It would be fair to say that interviews constituted the predominant method of collecting data, supplemented occasionally by documents regarding AML, and computer-based data in respect of AML cases. The use of unstructured interviews has proved highly fruitful in gaining considerable insights from the financial institution where the research was carried out. It has provided interviewees with both the necessary flexibility to reply to high-level themes around the difficulties they face within the domain of AML, and time to reflect on the complex nature of problems that arise when Information Systems are used for AML purposes.

Once specific themes of interest, which had direct implications on how AML was managerially handled by Drosia Bank, and which involved complexities that emerged from large-scale Information Systems, had been decided, then follow-up interviews were carried out that provided additional material. Such follow-up interviews on particular themes that had been chosen have been instrumental in uncovering insights that are elaborated further in Chapter V where the findings from the case study are discussed. All data collection activities took place within a 2½ year period, and hence the case study can be regarded as longitudinal. Beyond that period of time where the predominant data collection activities took place, there were a few occasions at the time of the writing the dissertation that a few clarifications were required (and indeed additional information), and to which the staff members of Drosia Bank kindly responded. Due to the confidentiality agreement agreed with Drosia Bank, it is imperative to stress that – during data collection – I was made aware of a multitude of high-profile and sensitive cases, along with the way they were managed by the Bank. Even though no such cases can be disclosed, the fact that the bank's staff were willing to discuss important details has greatly enhanced the researcher's understanding, and allowed him to reflect further on a multitude of aspects that touch on AML (ranging from collection and analysis of reports, communication aspects, training, determining suspicion, etc).

Indeed, besides being granted the opportunity to question personnel throughout the financial institution (and mostly within the ML-analysis team and the Compliance team) throughout the period of 2½ years, there has been a series of occasions when the researcher was given an office at the heart of operations of the ML-analysis team. From there he had the opportunity of direct access to the intranet of the financial institution (a computer was provided for that purpose), access to the special case management system software where all ML cases were recorded, access to a variety of other information systems, and perhaps most of all, the ability to observe day-to-day operations of the ML-analysis team with the possibility of interrupting and asking questions about particular items of interest. On some occasions documents were requested to supplement specific lines of investigation; on a multitude of occasions, staff members proactively suggested articles and publications of interest or internal documents and

guidelines that would shed light on some operational perspectives that were required to resolve issues surrounding data collection.

In the following table 3b, the reader can find a summary of both primary and secondary methods that were used in the process of collecting data for this dissertation. These are classified according to a qualitative/quantitative differentiation even though the line between the two is sometimes considerably opaque (there are occasions for instance when a single piece of evidence – such as an internal report – may include both):

Data collection methods	Qualitative	Quantitative
Primary Data collection	Unstructured Interviews, semi-structured interviews, direct observations, informal meetings	Statistics calculated with raw data from Case Management System (STRs analysis, branch reporting indexing)
Secondary Data collection	Internal reports, government and industry reports	Statistics sourcing from complementary evidence and secondary interviews[35]

Table 3b: Data collection methods used in this dissertation

[35] When an interviewee would for instance allude to a statistic that was neither part of a report or was not the result of scientific statistical analysis on the basis of raw data where access was provided

Applying Stage 3: Coding the Data, Applying the Theory, and Reaching Conclusions

a. Coding the data

In analysing mostly qualitative data there is an unavoidable process of categorisation that takes place where disparate 'data elements' are grouped together for the construction of arguments. This is known as 'coding the data'. As previously noted, this is done in distinct stages. Various researchers (Cooper and Hedges 1994; Coffey and Atkinson 1996; Berg 2001; Auerbach and Silverstein 2003; Richards 2005) mostly recognise this to be a 3-stage process (even though such a neatly defined delineation implies that interpretation and innovation in research can be clearly programmed, but this is a vast oversimplification):

i) Open coding: where the researcher starts with a broader research domain and a set of research questions. Open coding constitutes a first pass through the data elements that have been collected

ii) Axial coding: where categories have been defined within the coding process, and where the determination of these categories proceeds into elaborating the arguments that respective categories would support (while reflecting in their interconnections), and finally,

iii) Selective coding: where a last pass of incorporating further data elements takes place to corroborate the arguments.

In considering the aforementioned coding stages in the context of this dissertation, the following stages can be delineated:

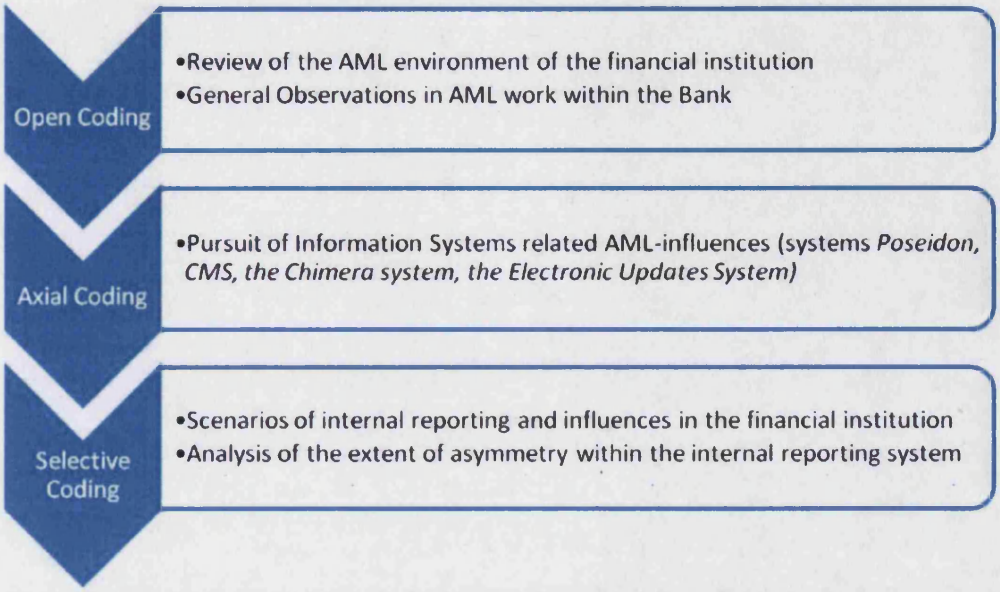


Figure 3.3: Coding stages

b. Applying the theory

According to Walsham, theory is both a way of seeing and not-seeing (Walsham 1995). Theory is simply a tool that mediates the interaction between the observer and the observed. Once the tool for mediation changes, so does the description of whatever is observed. It therefore becomes a question of appropriateness as to whether a theory used to study a context fits closely the observed phenomena. The theory applied in this dissertation is Systems Theory, in particular drawing on the works of Professor Niklas Luhmann (Luhmann 1990; Luhmann 1993; Luhmann 1995; Luhmann 1998; Luhmann 2000; Luhmann 2000; Luhmann 2002; Luhmann 2004; Luhmann 2005). Even though possibilities often arise in research for the application of more than one theoretical framework, the application of more than one theory does create confusion as there is always the additional problems of how well the theories match together, and the conflicts that may arise. While other theories have been considered in the context of AML, despite a somewhat theoretical immaturity of handling the topic, and because most research around AML revolves in the purely descriptive level, these theories are considered not to have the theoretical rigour of Systems Theory (Angell and Demetis 2005). While neo-institutionalism (Dimaggio and Powell 1991; Scott 1991; Scott and Meyer 1991; Zucker 1991; Scott 1994; Selznick 1996; Hasselbladh and Kallinikos

2000) was initially considered for the purposes of this dissertation, it was deemed insufficient to provide systemic insights for a holistic treatise of the AML domain. Indeed, a number of subtleties that surpass the purely institutional and embedded order of social and economic reality cannot easily be examined devoid of their systemic provenances or the systemic implications they give rise to. Considerations regarding the applicability of the theory chosen are further elaborated in the chapter dealing with Systems Theory.

Regarding the implementation and incorporation of systems theoretical ideas within the domain of AML, the researcher has previously published three theoretical papers informed by research that seek to combine Systems Theory with AML. In chronological order these have attempted to:

i) Provide the foundations of AML research on the basis of key systems theoretical ideas (Angell and Demetis 2005)

ii) Consider the systemic role of AML-related technologies, and how they have had an impact in the broader AML system (Demetis and Angell 2006)

iii) Reflect and deconstruct the risk-based approach for Anti-Money Laundering that has been introduced by the 3rd Directive, and inform the deconstruction by using various systems theoretical ideas on risk, and in particular those of representation, distinction and paradox (Demetis and Angell 2007)

Following a more elaborate treatise on systems theory, this dissertation intends – as noted in the research questions – to outline the core systemic differentiation of Anti-Money Laundering, to examine how technological consequences come to impact the domain of AML itself, and to investigate how AML can be viewed as a distinct system if it is to be studied properly in the systems theoretical sense. The interaction between these aspects is further informed by data collected mainly through the case study, and supplemented by various other resources.

c. Reaching conclusions

Based on the documents that have been collected and enriched by the data from the interviews, conclusions are subsequently drawn. That is, the analysis of the data proceeds through the lens of systems theory. It is important to realize that this is one of the most crucial sections, as the interplay between analysing the data through the theory and describing the subtleties in the domain through the research questions, must be balanced and carefully justified. It is also useful to reflect on the question of whether one really collects the data and *then* analyses. Sometimes, this process is reciprocal, meaning that the researcher asks his questions and formulates his hypotheses and descriptions, based on his theoretical framework. In that way, it is useful to consider if the *analysis* is actually also a part of the *data collection* through the interviews, and how that may restrict or enhance the further analysis of the data (and to what extent).

An equally important aspect that must be carefully thought through is that the very fact that the analysis takes place through the use of a specific framework; it is unavoidable that many factors that influence the phenomenon being examined are not considered. This is because the framework focuses the study on a specific array of factors that are subsequently examined. Therefore, to realize what factors remain out of the research process, and to describe them briefly without affecting the core of the analysis are also important. Not everything can be included through the interplay of analyzing data and theory, but after all, the point is to focus on these factors invoked by the data, and that the theory most closely describes. A convincing account of what must be given additional attention and emphasis in the research is what feeds back into potential theoretical and practical contributions.

In the chapter that follows, the theoretical framework to be applied is presented and the key concepts around it are analysed.

The whole is more than the sum of its parts"

Aristotle

Chapter IV: On Systems Theory

Chapter Structure

This chapter describes the key theoretical ideas around systems theory that will enhance the empirical data collected and presented in the case study in chapter V. 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.

Introduction

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 (not even Systems Theory) 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. 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, re-

construction, and application become severely dependent on the observers that employ the operations and conceptual schemas, which the observers themselves develop within particular circumstances and contexts.

Even though Systems Theory (ST hereinafter) has been in existence for decades, a series of paradigm[36xiii] shifts have occurred within the theory, which have influenced the theoretical concepts themselves. A detailed examination of such evolution is an elaborate task and well outside of the scope of this dissertation, as one has to go back almost 400 years in the history of the influences behind ST, and differentiate between 35 major figures in the construction of the theory that 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 (or rather co-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 created the aura of attributing the status of super-theory to ST, and even more so, to characterize it as a particularly impressive one[37]. One might initially be problematised with the attribution of a 'supertheory' status to any one theoretical construct; however, this is done in order to differentiate amongst several types of theories that can unavoidably be juxtaposed with ST. Whereas 'grand theories' appear to achieve the formulation of an all encompassing framework, and to seek 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).

For 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 considerably 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 systemic evolution) have all been

[36] The paradigm shift concept is found in Kuhn, T. S. (1970). The structure of scientific revolutions. Chicago, University of Chicago Press.

[37] This comment is attributed to Professor Niklas Luhmann in his work, 'Social Systems'

described through the use of the lexicon of ST, and the term supertheory 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 domains that differ considerably. This is particularly the case for financial systems and the economic functions that they seek to fulfill. 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 organisations (e.g. financial institutions), as the assumptions that organisations are simple and 'closed' systems (and that the environment within which they operate is stable) no longer holds true ... organisations 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).

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 field of Information Systems, which is multi-disciplinary in itself. Perhaps this could also help find an identity for the field of Information Systems, which has faced considerable crisis as to whether it even constitutes a distinct discipline (Avgerou 2000). Indeed, prominent scholars in the field have not refrained from suggesting that Systems Theory could bring out the full potential in Information Systems research by providing rigour and relevance, and that IS may even gain considerable new insights in the socio-technical sphere and within interpretivist research (Lee 2003), while at the same time recognizing that ST has already contributed considerably to the field of Information Systems (Xu 2000). In an era of increasing complexity in the implementation and implications of Information Systems, 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). It must be stressed, however, that as far as this dissertation is concerned, simplifications of the theory are not within its interests, and as such, Soft Systems Methodology (SSM) (Checkland 1985), which includes concepts from ST for systems analysis and requirements simplifications, is outside of the scope of this research, as the

concept of the system in SSM becomes considerably restricted (and rather confined to the technical realm).

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 (like Anti-Money Laundering). 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 to those who genuinely lack a belief that there can be a solution to a problem domain. 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[38] 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 problematisation, which must not be taken lightly. To think of Systems Theory as something like

[38] Quite often the result of positivist remnants in logic

mechanics, which provides answers to problems with the answer built-in in the form of particular laws that govern the behavior of systems, is a grave mistake (Arbib and Cornelis 1981). Equally it is argued in this dissertation that it is a grave mistake 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 de-contextualize the *importance*[xiv] of the observer, and tries instead to describe the problem domain (as viewed by an observer) and ultimately describe the significance and interdependencies of complex processes within the system, allowing them to be examined. In this manner, considerable insights can be gained by using the theory, but most importantly, it stresses increased vigilance into the systemic complications and implications that are entailed in decision-making processes (at any observer-level, e.g. 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[xv] (Crotty 1998). ST diverges from such an approach, by examining the system as a whole (*embracing holism instead*); 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*[xvi, xvii] which will be further analyzed 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', and 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 & Distinction

According to Professor Niklas Luhmann, 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 utilised for further exploration and analysis.

The start point of any systems theoretical analysis must be 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 (difference as a unity), the definition of any system would be impossible, thus rendering its observation infeasible. 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*[39] (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[xviii]) 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 observer-relative. 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[40]; 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',

[39] The existence of a *three-party duality* which in this case is (system-boundary, boundary-environment)
[40] Within the tradition of second-order cybernetics employed here

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 pre-requisite 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."[41] (Luhmann 2002)

[41] p. 87, chapter on the 'Paradox of Observing Systems'

As the above assertions about the construction through observation 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 dissertation moves on to discuss the concepts of the system, boundary and environment, the aforementioned comments should be kept in mind.

The System

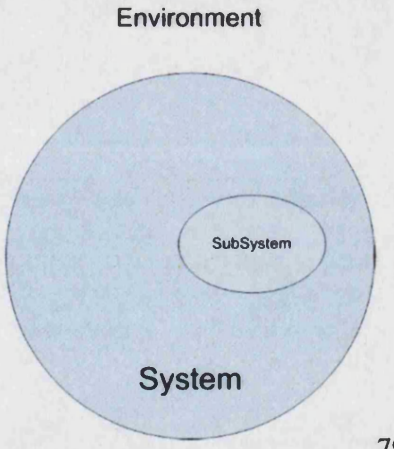
There are two important ways in which we can describe just what a system is. It is important to note here that any systemic description and observation must conform to the fundamental axiom of *distinction* that is constitutive of observation. In other words, in order to 'see what is inside' a system, 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:

i) A system is composed of subsystems

ii) 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 system/environment relations within it.* Even though diagrams 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 – that between system/environment – 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? The logical answer – guided by differentiation – **would be no***[42]*. 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 realise here that first and foremost this is a matter of observation, and that the definition of the system guides this process, for it is only in this scenario (upon system definition) where system/environment esoteric differences can be realised. The difference in internal system/environment relations (of an esoteric type) 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, without which the system would not have been created (or identified by an observer)*. 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 realised 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

[42] To some this initially appears counterintuitive however the reason becomes evident once one considers the relations between systems and complexity.

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 of the problem, 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, the dissertation now turns 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 the Systems Theoretical perspective and refers to the enumeration of elements. To illustrate this critical point that is found in many different types of systems, the example of the human brain[43] 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 100billion, it becomes obvious that put

[43] The first time I heard this example was when studying Physics at the University of Crete. I attribute this to Professor Gregory Psaltakis who described the example in his course on Quantum Physics and then at a conference on the Quantum Mechanics of the Brain with Dr. Dimitris Nanopoulos as speaker.

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 (Aristotle 1957). 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, and dependent upon the synapses or connections that are 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 from which emergence propagates. As the eye cannot see itself seeing, self-observation regarding the attribution of emergence within the system itself has to remain inconclusive. Far more important is the recognition that there are indeed *emergent phenomena,* a set of properties that are *based on, yet emerging from the* systems' 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 pre-conditioned 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 – through an extensive analysis – is that 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 systems' 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 the system itself[44] – 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 wasn'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

[44] A distinction that I have come to call self-referential differentiation

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. The reason 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 a 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 – through self-organization and improved communication amongst their subsystems – *increase their sensitivity* to boundary feedback, and thus partially 'control' the interaction with the environment, but without this implying 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 a necessity for structural coupling between the system and the environment, and refers **to the exchange of codified information being transmitted between the two.** From the systems' perspective, this feedback can take two distinct forms, namely *positive* and *negative* feedback.

Positive feedback affects the system in a distinct way and ultimately threatens the system's existence[45]. 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 a recognition of a temporary state of the system that is used by to monitor minor variations in the system. 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 sub-systems 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 sub-systems as a new system, or it can lead to extinction, especially in cases where there is little unity of purpose among the sub-systems. 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 sub-systems will survive the forceful processes that occur within the system, and how they will change it. Sub-systems 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.

[45] The word 'positive' here does not imply that the feedback is favourable for the system, but quite the contrary.

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[xix].

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 dissertation, 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 complexity and its consequences; for complexity is not a methodology, but a way of thinking (ibid); and one that has been used extensively in Systems Theory as an important property of systems. In this regard,

Social Systems and Socio-Technical systems do exhibit complex characteristics for a series of reasons and descriptions that will be further discussed below.

But why is there such a thing as complexity? There are several reasons that point towards acknowledging its existence. The most important one 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, computing, etc, 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 (Kallinikos 2006).

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. Within such a setting, technology becomes crucial, as complex technologically based processes supporting Anti-Money Laundering create a series of systemic phenomena within AML itself, which require 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 dissertation, 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-organisation, connectivity, feedback, co-evolution, etc.

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) – *emphasis added*

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[xx]. 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 and they enable a containment of contingency that allows the development of communicative contexts that are particular to each system (ibid).

Here we reach another key point: observation implies a 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; Luhmann 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 inter-related in systemic formation, it is time to move on to a discussion of self-reference – a key concept within ST[46] –, and thereby gradually close this chapter.

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 spectacular and 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 – many years later – 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 (e.g (Ashby 1958)) and in particular, second-order cybernetics (Korzybski 1948; Von Foerster and Josiah Macy Jr. Foundation 1950; Von Foerster 1951; Von Foerster, Zopf et al. 1962; Bateson 1972) that already included concepts of control and communication, learning and adaptation, evolution, and most closely, *self-organisation* (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. The word itself comes from the combination of two Greek words, namely αυτο (auto – meaning self) and ποίησις (poiesis – meaning *to make*). 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

[46] And one that has become Luhmann's core concept in the design of his theory for social systems

elements, thereby re-constituting their functioning parts. This presented a most notable and crucial connection in Biology where that Maturana and Varela made the connection with the the idea of self-organisation.

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 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 below, that of the Klein Bottle.

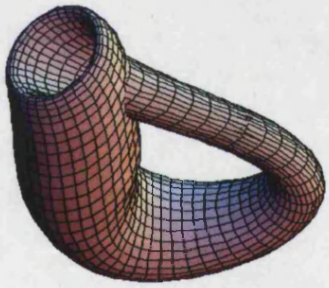


Figure 4.1: The Klein Bottle[47]

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 *systemic self-referential* processes that have the potential of increasing 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 causalities. In this manner, self-

[47] Reproduced with the Mathematica© Software Package (Wolfram Research)

reference can also be recognized as the crucial mechanism with which the system reduces environmental complexity.

The literature predominantly distinguishes three meanings that 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 dissertation 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 hopefully becomes clear that self-reference implies more than a mere reference of the system to itself. If that were the sole 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:

i) 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).

ii) 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 ~ e.g a policy that has been used before, or a particular course of action, which is pre-decided when confronted with similar environmental events).

iii) Self-reference as fundamental for Information Processing, whereby the system refers to itself by interrogating those elements that are 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 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, it 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 inter-related 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. Let us provide an example from the field of sociotechnical studies and 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 is used to produce other technology in various forms (a self-referential process in itself), and just as a social system re-produces itself, so too does the information systems. 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 it, 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).

We therefore 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, and typical of how the term *system* has been commandeered from its distinct theoretical provenance.

Still, as argued in previous paragraphs, self-reference can be found at any systemic level once a system is identified by an observer. 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 was deliberately chosen from outside the core topic of this dissertation[48] even though it needs to be emphasized in advance that when technology is viewed systemically then the term self-reference

[48] But within the researcher's interests through the FIDIS project of the European Union

acquires broader characteristics. Nevertheless, an initial example is useful to clarify the mechanism of (self)-reference within technology.

The example concerns a pattern recognition algorithm, that when presented with a handwritten image, returns two probability values, real numbers between zero and one. A series of 5000 images – 10 sets of 500 images (one set for each numerical digit between 0 and 9) - is processed, and the output is represented graphically in figure 4.2. Each set is drawn in a different colour – handwritten versions of the digit 2 for example are drawn in green. The algorithm's two output parameters are interpreted as a two-dimensional Cartesian coordinate within a unit square; each of the two mutually perpendicular axes representing one of the algorithm's output parameters. Each of the 5000 images is then scaled down (so that at the resolution of figure 4.2 it looks like a dot) and drawn at its coordinate position. The basic shape of each of the ten different digits, that enable us to differentiate between digits even when badly drawn, tend to cluster each of the ten sets in different regions of the unit square. Variations in handwriting cause the scattering within each cluster – if 500 images of the same typewritten digit were processed (such as the digit 2 shown in figure 4.4), then the corresponding dots would be more or less superimposed. Hence the resulting figure looks like ten clusters of different coloured dots. Zooming in on the predominantly green portion of figure 4.2 results in figure 4.3.

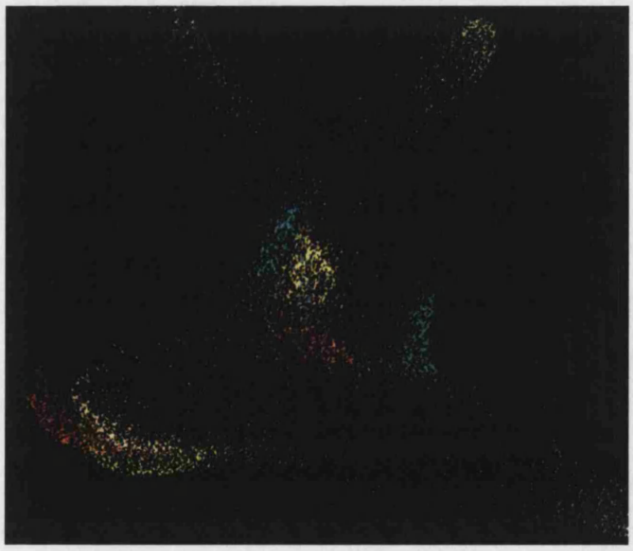


Figure 4.2: Pattern Matching, Visual Representation and Scattering

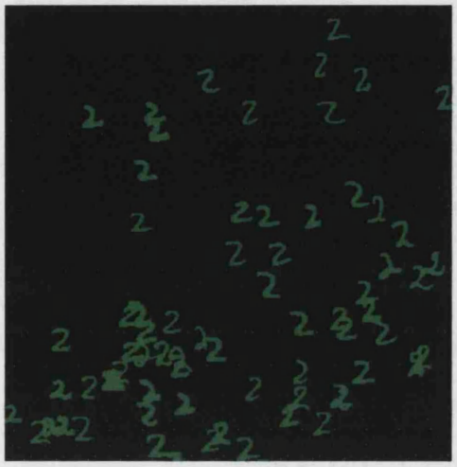


Figure 4.3. Scattering of 2s according to probabilities

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. From the figures displayed above, and through the accompanying description of the aforementioned example, this conceptual delineation would take the following form: the instances would refer to all individual images containing 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 (i.e. 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 two.

The function that technology comes to fulfill 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 a 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 examined instance (say any number from 0...9 according to the pre-defined 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 500 instances of the 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.

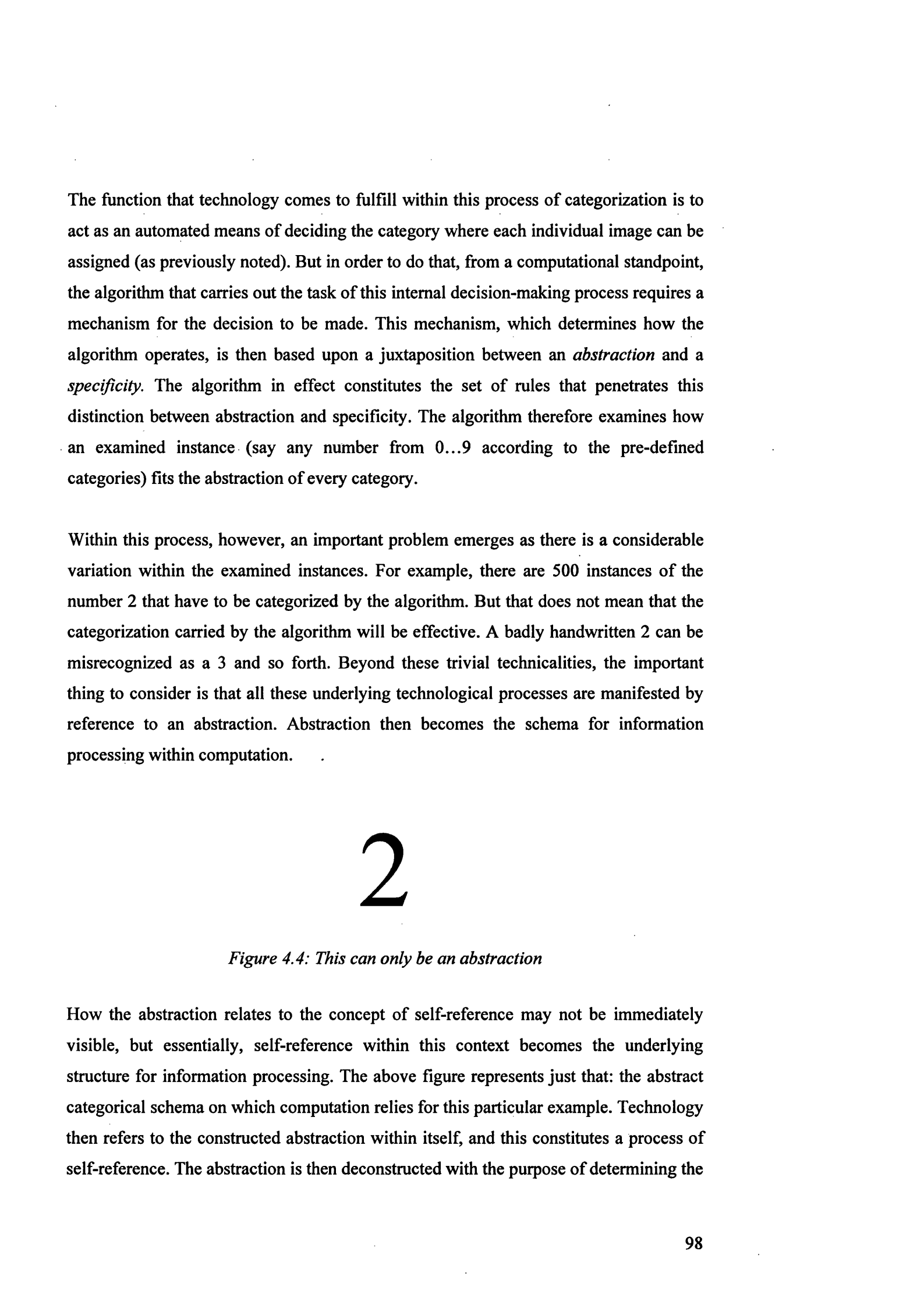


Figure 4.4: This can only be an abstraction

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. The above figure represents just that: the abstract categorical schema on which computation relies for this particular example. Technology then refers to the constructed abstraction within itself, and this constitutes a process of self-reference. The abstraction is then deconstructed with the purpose of determining the

abstraction's informational 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:

i. The representation of abstraction has to be deconstructed and this causes difficulties with incoming instances (e.g. Figure 4.4. that represents the abstraction of number 2 deconstructed by an algorithm; that deconstruction essentially determines what is a 2 in pattern matching according to the computation. Since different values may be given to analyze the ideal curvature of lines of the number 2 in its shape, etc., this implies that the abstraction of the number 2 that is computationally deconstructed can have a variety of representations).

ii. For the example of pattern matching, the incoming instances have to be recognised 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.

iii. 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 was not pattern matching digits, but instead simulating money-laundering behaviour, then the underlying computational process would exhibit the same foundational properties. In the laundering example the abstraction of a number is replaced by that of a model 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, etc[49]). Finally, the instances within the categories (in the former example these were the variations of a category – e.g. 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 in the hope that suspicious transactions are 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 scattering, a similar kind of variation displayed in Figure 4.2, but this time it concerns 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 utilised and hence all information processing becomes self-referential.

The above example, technical though it may look, points towards a crucial aspect in self-reference that should be emphasized: *self-reference has nothing to do with tautology, for 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, for 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

[49] These are some of the most commonly used parameters in profiling money-laundering through technology

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[xxi].

Later in this dissertation (following the description of the case study) further discussion and examples[50] 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 identified system that can be pre-supposed or observed. 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.

[50] Examples that I have come to realise, construct and delineate through my participation in two European Union projects related to Anti-Money Laundering (Projects SPOTLIGHT and GATE)

"The learning and knowledge that we have, is, at the most, but little compared with that of which we are ignorant"

Plato

Chapter V: Empirical Findings – The Case Study

Chapter Structure

This chapter discusses the main findings from the case study that was carried out over a 24-month period in a Greek Bank. The chapter starts with an overview of the Greek Anti-Money Laundering system within which the Bank operates, and will contribute to the reader's understanding of some critical, but perhaps contextual examples that will be given in due course.

Following the brief introduction of the Greek national AML system, issues of access to the Bank are discussed, along with an overview of what data was made available to the researcher. This is followed by an analysis of the internal reporting system of the bank, and an analysis of the increase in the number of suspicious transaction reports. The AML system of the Bank is then analysed in detail, based on 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 on 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, namely a Case Management System (CMS), whereby data is stored for all money-laundering investigations, and the POSEIDON Information System that is used to identify customers uniquely.

The Greek AML system

As a full member of the European Union, Greece has already taken the initial step of introducing a Greek Law for the prevention of money-laundering[51][xxii], based on the 1991 EU Directive on ML (EU 1991). Even though the adoption of the 1991 Directive came with a four-year lag, the Greek law has extended several aspects of the 1991 EU guidance by including additional crimes in connection to money-laundering, such as blackmail, fraud, theft, illegal trade of antiquities, embezzlement, , etc. A series of Banking Directives from the EU have also been implemented, and transformed the Greek financial environment from a strictly regulated one, to a financial system more open to competition and hence, more risk (Goldberg and Pantos 2003). Despite the fact that Greece is not a major financial centre, it remains true that due to the country's geographical position (at the southern end of the Balkans) as well as a remarkable geographical fragmentation that includes more than one thousand islands, it is very difficult to control drug-trafficking and smuggling of various forms.

Ten years after the first EU Directive on Anti-Money Laundering, the European Union issued another Directive in 2001, and although the deadline for its incorporation into national legislation December 2002, Greece did not take steps soon enough to implement it. Such an additional delay in complying with EU Guidance has resulted into some tension between the EU and Greece, with the former discussing a referral of Greece to the European Court.

With the European Union quickly responding to the global changes in Anti-Money Laundering, and the proposed 3rd AML Directive (EU 2005), Greece moved towards a draft law that would revise the previous law and incorporate the necessary changes for both the 2001 Directive, and the 3rd AML Directive. The revised law has been the subject of much discussion in the country, as several articles within the law have exceeded the requirements posed by the EU level, and have resulted in legislation that

[51] Law No. 2331/95 (Amendments: Law No. 2515/1997, Article 6)

was characterised by many as draconian. Two major changes in the revised[52] legislation included jail sentences for bank employees, and a considerable reduction of the threshold for reporting suspicious transactions on money-laundering.

There are a few things worth mentioning concerning the revised Greek Law on money-laundering in order to exemplify the issues mentioned above. The first one concerns the possibility of jail sentences for bank employees – up to 2 years – a sentence that was characterised as mild by the regulators themselves. With the introduction of such a penalty, the bank employee had to face the potential of a jail sentence even in the case where money laundering has taken place due to an employee's 'severe negligence'. In the past, jail sentences used to require proof beyond doubt that the employee was involved in money laundering. Furthermore, as the definition of money laundering in the revised legislation was expanded into both criminal and domestic law, a surprising legislative contradiction has emerged; whereby the money launderer could be charged with an offence of a low-value crime resulting from a small violation of the domestic code, and facing a jail sentence of six months; however, the bank employee who accepted the proceeds of this crime is facing two years in prison. Considerable changes have also occurred in terms of the definition of thresholds, whereby any criminal act (either penal or domestic) that results in financial proceeds in excess of €4,000 would be considered as money laundering. Such a change clearly constitutes a great shift in the Greek AML system, and is a big expansion in the definition of money laundering. Serious problems are posed in terms of implementation; and the potential effects of these changes on the national reporting system of suspicious transactions will take years to unravel. Taking into consideration that tax evasion is included as one of the crimes for money laundering, further problems emerge as financial intermediaries are burdened with the task of checking the tax obligations of their customers, something that goes outside of their scope, role, and functionality.

Also, contrary to other EU countries (e.g. UK) or the US, when a financial institution in Greece receives a fine for non-compliance of AML regulations, the size of the financial fine imposed by the Central Bank of Greece is not made public. This in theory may

[52] The revised legislation goes by the name of '*Modification and revision of articles of the Law 2331/95 and compliance of the Greek Laws to the Directive 2001/97/EC of the European Parliament and Council for the prevention of the use of the financial system for the purposes of legalising proceeds that source from criminal activities*'

have two direct consequences: first, since the financial fines for non-compliance on AML are not made public, then the financial institutions upon which the fines are levied have no fear of reputational risk emanating from it. As a further and complementary consequence, non-compliance is not signalled to the market, and therefore further detrimental economic effects are not realised[xxiii]. In aggregated form, however, the press has learned that a total of seven financial institutions were fined a total of €1.87million for non-compliance against the Greek Law on the prevention of money-laundering[53].

After the introduction of the Greek legislation, two additional steps improved[54] the country's stance on AML. The first one was the constitution of a Financial Intelligence Unit (FIU), otherwise known as the Committee[55]. The Committee has the task of collecting, assessing, and investigating the reports from suspicious transactions. The committee's meetings are presided by a judge or public prosecutor, and members range across senior officers of the Ministry of National Economy, the Ministry of Finance, the Bank of Greece, the Athens Stock Exchange, and the Hellenic Banking Association. The Committee, also called the 'Competent Committee' in the legislation, may enjoy confidentiality and trust, but certainly not admiration in terms of its efficiency and working structure. The latter is often viewed as overly bureaucratic, while the members of the committee are seen as people who have 'nothing in common with each other, and in any case no expertise or training on Money-Laundering issues ... This poses an obstacle rather than an incentive to the AML efforts. It is worth mentioning that upon receiving a suspicious transaction report, the reaction time of the Committee upon receiving a suspicious transaction report is about one week before even referring the case to either the public prosecutor or to the SDOE[56], who for their part have also the task to investigate before taking any effective action' (Katsios 1999).

As well as setting up the Committee, another extremely important step under law 2343/95 was the creation of a Unit responsible for combating Financial Crimes. The Financial Crimes Enforcement Unit (SDOE) has the task of enhancing coordination

[53] http://www.in.gr/news/article.asp?lngEntityID=723290

[54] This is not a value-judgment here. Improvement refers simply to the critical aspect of constituting an FIU where none existed before.

[55] Constituted in article 7 of the 2331/95 law

[56] SDOE is dealing more broadly with economic crime in different forms, tax-evasion, etc. At the Committee for AML there is always a SDOE representative

between different agencies, and investigating financial crimes stemming from drug trafficking, weapons trade, etc. The Unit started its work in 1997, on a wide range of financial crimes, including money-laundering.

Banking supervision in the Greek financial sector is carried out by the Central Bank of Greece (BOG hereinafter), in full accordance with the Basle Principles and all other international standards. The BOG is also responsible for supervising the sound and efficient implementation of the FATF recommendations, and of course, for imposing fines in cases of non-compliance.

All of the above initiatives, along with the setting up of both the Committee and the Financial Crime Unit, demonstrate the country's intention to participate fully in the fight against money-laundering and to adhere to international standards. Even so, new risks are appearing, despite the fact that Greece could not be described as a major financial centre. This is due to the country's geographical location, the immigration problem, which has intensified, and an increase in drug trafficking. Consequently money-laundering is becoming an increasing concern (State 2001). Drug trafficking for instance, has increased dramatically within the last 5-7 years, as drug offences have almost tripled[57] (Interpol 2002).

Access to the Bank

Before moving on to describe the main findings of this case study, the researcher – once again – expresses his gratitude to all the staff members of the bank for their support, cooperation, patience, assistance and helpful remarks. They have always been truly wonderful and supportive of this effort and provided a wealth of useful information. Confidentiality agreements do not allow the exposing of either the names of employees or the name of the bank being researched; these legal and ethical obligations are honoured throughout this document.

[57] The connection between an increase in drug trafficking is not clear, although it is commonly assumed that it accounts for 80% of the money being laundered.

First of all, the name of the bank has been changed to that of '*Drosia Bank*'. Even though the topic of Anti-Money Laundering involves internal working processes of high confidentiality for obvious reasons, the researcher was granted an unprecedented level of access whilst conducting the research. This included access to:

1) The 'Know Your Customer' Policy of *Drosia Bank*
2) The bank's 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 Greek FIU[58]
6) Access to the Case Management System of the Bank where all cases concerning money-laundering are recorded
7) Statistical data concerning the whole branch network of *Drosia 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[59] 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
12) The Fast Transmission of Electronic Messages (FTEM[60]) System
13) The Electronic Updates System (EUS), which is used to inform electronically tellers and other personnel
14) The TEIRESIAS online system where banks share information between them

[58] In the Greek AML system, a report has to be authorized by the MLRO before being forwarded to the FIU, an approach that differs from one national system to another *(in the UK for instance, members of money-laundering analysis teams can file a report directly to National Criminal Intelligence Service, and more recently to SOCA replaced NCIS)*

[59] Yet another fictional name

[60] Fictional name for the Information Systems platform that the MLAT uses to communicate with branches

15) Online Training Material

Besides documents, a series of semi-structured interviews were conducted with various stakeholders from *Drosia Bank* as well as other institutions, with the purpose of identifying systemic effects in the Greek national AML system. These include series of in-depth interviews with:

1) The Money Laundering Reporting Officer of the Bank

2) The Money Laundering Analysis Team (MLAT[61]) of the Bank
   a. The Manager
   b. The Assistant Manager
   c. Personnel working in MLAT

3) The Compliance Group of the Bank

4) The Information Systems Analysis, Design and Management team of the Bank
5) The Hellenic Banking Association
6) The Central Bank of Greece
7) The Ministry of Finance
8) The Financial Intelligence Unit of Greece also known as 'The Committee'

The largest number[xxiv] of both semi-structured and unstructured interviews was conducted with the MLAT of *Drosia 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 Greek FIU. Also, MLAT alone has access to the Case Management System for recording suspicious transactions in respect of money-laundering.

[61] Not to be confused with the term Mutual Legal Assistance Treaty

Drosia 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 Greece. It has swiftly reacted to improving its internal procedures and working processes for AML from the very first introduction of the Greek Law concerning money-laundering[62]. Two important related policies were introduced, one on 'Know Your Customer' rules and the other 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, and emphasis is given to several issues, such as customer identification, suspicious conduct, and suspicious transactions, etc. The policy outlines the importance of such identification every time a Bank-customer relationship is established, as well as stressing the collection of sufficient information for the development of individual 'transaction profiles' for customers[xxv]. 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. 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. It is worth noting here that according to Privacy International[63], Greece came first in the national privacy rankings for the year 2007.

---

[62] Law 2331/95

[63] http://www.privacyinternational.org/

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 attractive (in financial terms) 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 re-instates the importance of KYC, thoroughly analyzes 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 introduces fundamental issues surrounding AML, discusses what day-to-day operations require protection from potential abuse by money-launderers and it emphasizes compliance with current legislation. The policy stresses that every effort should be made to report any suspicious activity that is detected, so that the financial institution has the option to examine it further (through the specialised team working on money-laundering) and potentially to report it to the Financial Intelligence Unit.

Compared with the other Greek banks visited by the researcher, a considerable number of employees have been hired for the analysis and investigation of suspicious transaction reports. This particular bank was chosen as a case study as a result of initial interviews of Money-Laundering Reporting Officers from nearly all the major banks in Greece.

Increased vigilance on money-laundering, the introduction of AML procedures, policies and guidelines within the bank, and the training of personnel have also brought about significant changes in the reporting of suspicious transactions. As demonstrated in Figure 5.1 below, throughout a five-year period the bank has seen an important increase in the number of STRs received by the Money-Laundering Analysis Team.

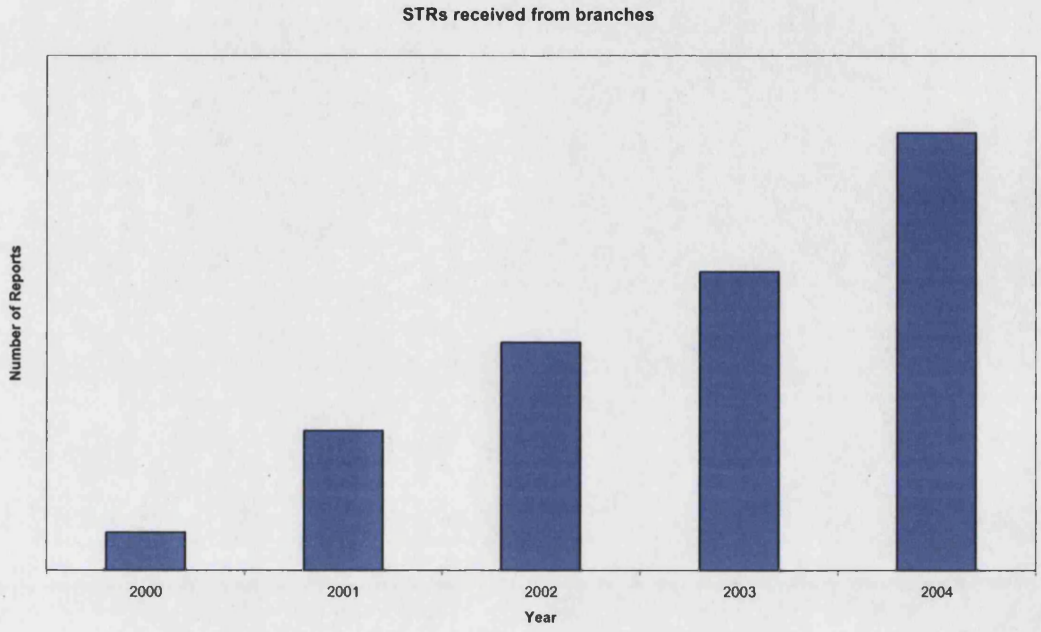


Figure 5.1: Increase in STRs[64]

In order to accommodate for such a change in the volume of suspicious transaction reports, the bank has recently decided to employ even more staff within the Money Laundering Analysis Team. As the trend is likely to continue, a simple statistical analysis was carried out for investigating the increase so far. This is demonstrated in the Figure 5.2 below for which the Money Laundering Reporting Officer made the following comments:

> "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 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"

[64] Numbers on the y-axis that could potentially identify the bank have been removed. It is the trend of increase that is of interest here; not the numbers themselves.

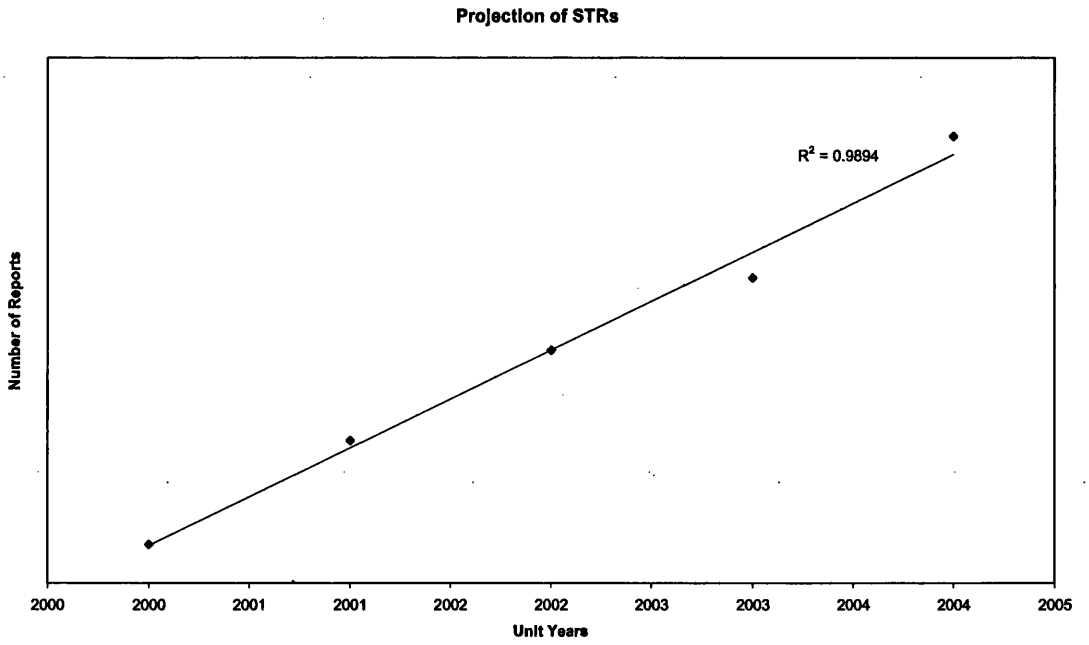


Figure 5.2[65]: Linear fit of STR-projection

As with the previous figure, actual numbers from the y-axis have been removed; only the general trend of increase is of interest.

Such an increase has become the source of a variety of problems in terms of investigation, and has brought to the surface subtle issues 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 five-year period, the percentage of reports that were deemed suspicious and worthy of reporting to the FIU became gradually disproportionate. Therefore, as the trend of the number of STRs increased, the percentage of STRs that were submitted to the FIU tended to decline!

Figure 5.3 below deserves particular attention. In the year 2000, nearly 73% of the STRs received from staff reports were forwarded to the FIU after investigation from the

[65] Best fit in the graph was calculated with the method of Least Squares. The R-squared value is the relative predictive power of a model. The R-squared can take a maximum value of 1 if the linear approximation is a perfect match with the empirical data. In this scenario, with a value close to 0.99, the approximation is surprisingly good and the result disturbing for the MLAT if the trend does not face a discontinuity.

MLAT. That number reached the peak of 84% in the year 2001, while in the year 2004 the percentage of STRs that were forwarded to the FIU had dropped to 28%!

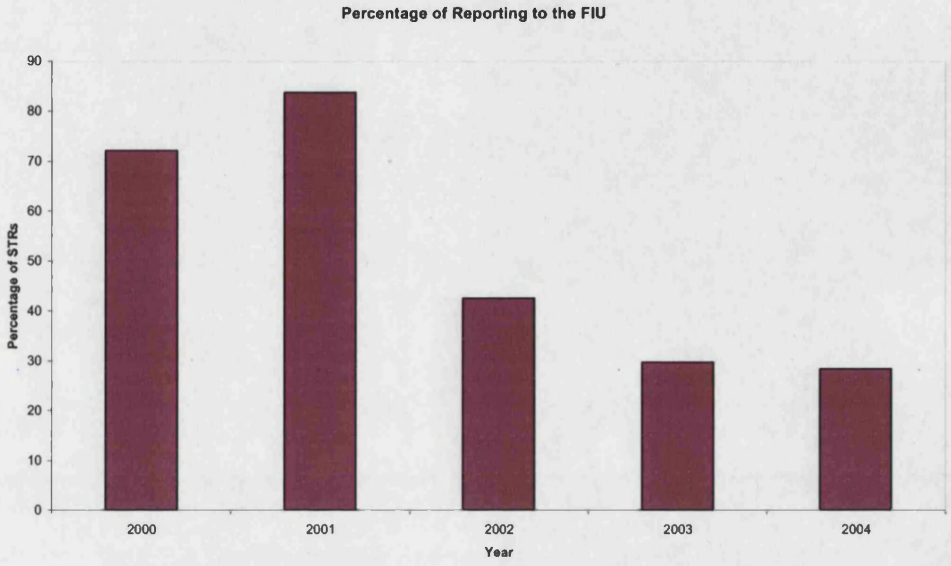


Figure 5.3: Reversion of reporting

Juxtaposition between figures 5.1 and 5.3 demonstrates a clear trend of disproportionate reporting from staff members of the bank's network when compared with the reports that are actually deemed suspicious after further investigation and forwarded to the FIU. Following this finding from access that was provided to statistical data, and following discussions concerning the above finding with several interviewees, the following observations and comments were carried out:

a) 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 the Money-Laundering Analysis Team. ***Fear-compliance*** along with potential fines from the supervisory authority also played a role in such a high percentage of reports being sent to the FIU.

b) The sudden drop in the reports sent to the FIU between 2001 and 2002 (84% and 43% respectively) reflects a change in senior management and a new line of action. The MLAT was encouraged to

be more cautious, to refrain from reporting nearly everything, and to focus on those cases that were worthwhile reporting (where there was serious suspicion for actual money-laundering going on). Complementary to this change in the internal policy of the bank, it is worth noting that the Greek FIU had also contacted the bank informally and urged it to submit fewer STRs as the volume of reports from the totality of the Greek Banking system was clogging the processing capacities of the FIU, and was creating a backlog.

c) Despite the increase suggested from figure 5.1, 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 surprisingly stable from 30% in the year 2003 to 28% in the year 2004.

In respect of point c), even though a full explanation for such stability in times of change and where a multitude of factors come into play cannot be attempted, there is an underlying qualitative aspect that underpins such a condition. That aspect is of systemic nature and associated with every *system's internal capacity* of interconnectedness, and particularly its *information processing*. Once a system reaches a certain degree of organisation, then the *internal quality that characterizes its information processing capacities does not usually deviate much from the norm.* This having being said, a more detailed analysis on such systemic implications can be found in the Analysis Chapter.

AML within the Bank

There are predominantly two mechanisms that influence the work of the money-laundering analysis team of the *Drosia Bank, namely:*

1) Investigations on money-laundering that start with a request from the FIU or a public prosecutor

2) Investigations on money-laundering that are initiated by the network of branches of the bank via the traditional route of filing an STR

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 Anti-Money Laundering domain.* The problems that usually emerge at a systemic level, (an analysis of which is provided in the Discussion 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:

Examining Scenario 1

Quite often, the Greek Financial Intelligence Unit or a prosecutor will request information from *Drosia Bank* on investigations concerning money-laundering. Such requests typically require the provision of transaction-data from the Bank. Sometimes these requests are limited to transaction data for a period of 5 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 (MLAT hereinafter), and then forwarded appropriately within the bank. The first source of retrieving such data is the *Automated Centre for Transaction Recording* of Drosia Bank, which restricts itself to providing transaction data 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 centralised 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. Even though the FTEM system has a facility through which the input of standardized text is allowed[66], this is one example of an option that is not currently being utilised. Furthermore, the requests received by the FIU are never sent in an electronic format, and therefore duplication of work becomes – to a great extent – unavoidable. In cases where many names are being investigated along with their details (National Identity Numbers, etc), this becomes a considerable effort[xxvi].

Once an employee 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 at the level of an individual branch to the FTEM is gained by either the Manager of the branch or the Chief Teller, and 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

[66] By using Macros so that initial details are already recorded and used

where the data are available in transaction slips, the employee will collect *all the slips and manually handwrite all the transactions – one by one – 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 becomes then 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.

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 data-sets. 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 Greek 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.*

The Greek FIU uses similar methods of communication to the totality of the Greek banking sector, 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.*

The Greek FIU subsequently relies on a manual examination of such transaction data before forwarding to the prosecutor. Taken that the FIU currently employs a maximum of ten people (along with a few assistants), it becomes clear that a thorough investigation of all transactions is rendered difficult just by the volume of the documents collected alone. 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, things get even more complicated.

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[67].

Examining Scenario 2

The second distinct way in which an investigation concerning money-laundering takes place is via the traditional route; that 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, and which is based on the guidelines issued from the Central Bank of Greece (BOG). These guidelines make use of typologies that

[67] For example, in a recent investigation there were so many transactions involved that it would be impossible and would probably burden the authorities if the bank were to send all data irrespective of amount. This was discussed and it was finally agreed that only those transactions that were above €1,000 would be forwarded.

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 often 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 extensively 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. A record of what person is assigned which investigation is kept by the manager of the MLAT, so that the work is evenly distributed and no one employee is burdened with more investigations than any other.

Every single STR that is received from the Bank's network is logged on an Information System that is a basic *Case Management System*[68] (CMS hereinafter) and a simple facility that the software provides is used to extract statistical information from the reports being investigated. Reporting statistical information from *Drosia Bank* to the supervisory authority of the Central Bank of Greece is compulsory and takes place annually.

[68] Thanks to the Manager of the MLAT, I have also received the full manual of the Case Management System that the team uses, describing every single work flow and potential of the software. Whilst such extensive details cannot be disclosed, they have greatly contributed to my own understanding of the internal processes involved.

The CMS was installed in 1999, when most Greek banks 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 fair to say, the CMS system has become the main companion for work of the MLAT team within Drosia 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, and this resulted in the creation of a software package with few capabilities, stringent processes, and inflexible controls. Requirements specification was unfortunately 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.

The semantics of the software's name also play an important role, as the software itself claims to be a tool for the *electronic processing of suspicious transactions.* Far from being an automated tool that monitors electronic transactions, and far from being a profiling tool for modelling money-laundering 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 in'. 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. 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 more than five years 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[xxvii] 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. Subsequent investigations however about the *same* people would have to be inserted into the CMS with a different unique number, thus increasing the information complexity of individual cases, and compromising the usability of the software and the data retrieval 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 *per se* has resulted in a failure; quite the contrary. The POSEIDON system itself is fully operational up to the time of writing, 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. "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 company operating in another EU country. 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,* and perhaps more importantly, *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[xxviii] 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 (UIN henceforth).* The system has various features that show the overall position of the customer, such as account information, deposits, withdrawals, etc. 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 lengthy process, one immediate consequence that stemmed from the creation of highly complicated informational infrastructures was the difficulty in maintaining consistency in the database format. The different information systems were far from uniform. New technologies were constantly being developed, and as new 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 *Organisation 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 system has been constantly misused (and continues to be so) 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 UID 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 *Drosia 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 recognised the problems with POSEIDON, a decision was made to make consistent attempts at rectifying them. It turned out that the branches would be burdened with clearing out the underlying complexity; a complexity to which they themselves had greatly contributed[69]. The *Automated Centre for Transaction Recording* would then query its own databases[xxix] 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 cross-check the identification documents from the customers, and proceed into uniting the different accounts under a single POSEIDON identification number. The instructions that were given to staff members would also include collecting the required information missing from the POSEIDON system. This additional information (e.g. postcode, occupation) was needed so that the database was as complete as possible, with the ultimate purpose of creating a single POSEIDON Identification Number in those cases where multiple accounts existed.

According to estimates given to the researcher by the Department of *Organisation 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% 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% of the customer base had a unique identification number.

The implications for the Money Laundering Analysis Team were clear. Considering that POSEIDON is the only online system to which the MLAT has access[70], 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

[69] Describing this whole story somewhere else (conclusions) – as a self-referential process of correcting/injecting problems into the system itself

[70] Apart from the TEIRESIAS system which links all banks for a different purpose

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.

In any event, the identities of those under investigation by MLAT for money-laundering are cross-checked in POSEIDON. Establishing the identity of a person under investigation becomes then 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 informational decentralisation, 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[71] by making use of POSEIDON as it is incomplete. 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

[71] Obviously this only applies to the cases where the FIU requests information

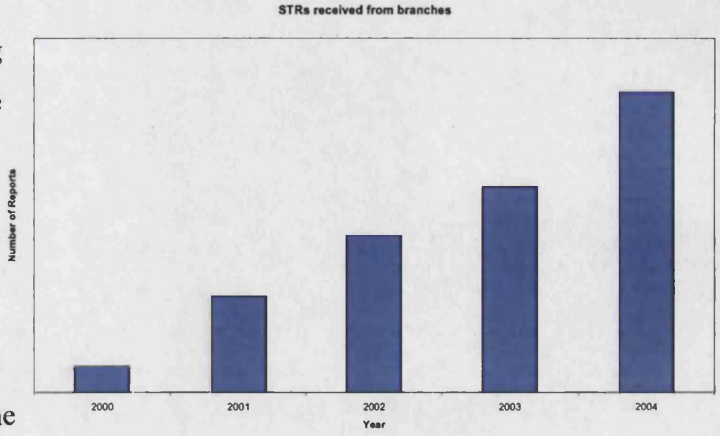
occasions a very time-consuming process, something that is critical in cases where money-laundering has potentially taken place".

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 utilised for and crucial to money-laundering 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, 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 subsequently 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.

This section proceeds by placing even more attention to confidentiality issues. Any characteristics that may have exposed the bank throughout this analysis have been removed or generalised so that the bank is not identifiable. Attention to preserving confidentiality has not however jeopardised presentation of the findings. What is presented in this section is both typical and statistically representative of the entire branch-network of the bank.



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 last few years. 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 (i.e. geographical distribution, etc) 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 information and 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 their 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[72] with which the following results were produced.

Figure 5.4 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 y-axis[73] 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.

Figure 5.4: STR-submission asymmetry in the branch network

From the above graph, 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

[72] For this data-mining platform (DataDesk v.6.2) and the feed of ASCII data into it, I have to thank Dr. Carsten Sorensen from the London School of Economics for his help, introduction to the software, and assistance.

[73] Hence such a big difference in reporting is not attributable to geographical factors.

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 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, 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):

i) To identify the percentage of the branches that – in the course of their existence within the network of the bank – have sent **no suspicious transaction reports whatsoever,**

ii) To identify the percentage of the branches that have sent very few STRs,

iii) To identify the pattern of distribution that stretches from those *groupings 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 categorisation of branches **with the same number of suspicious transaction reports;** this produced the following graph:

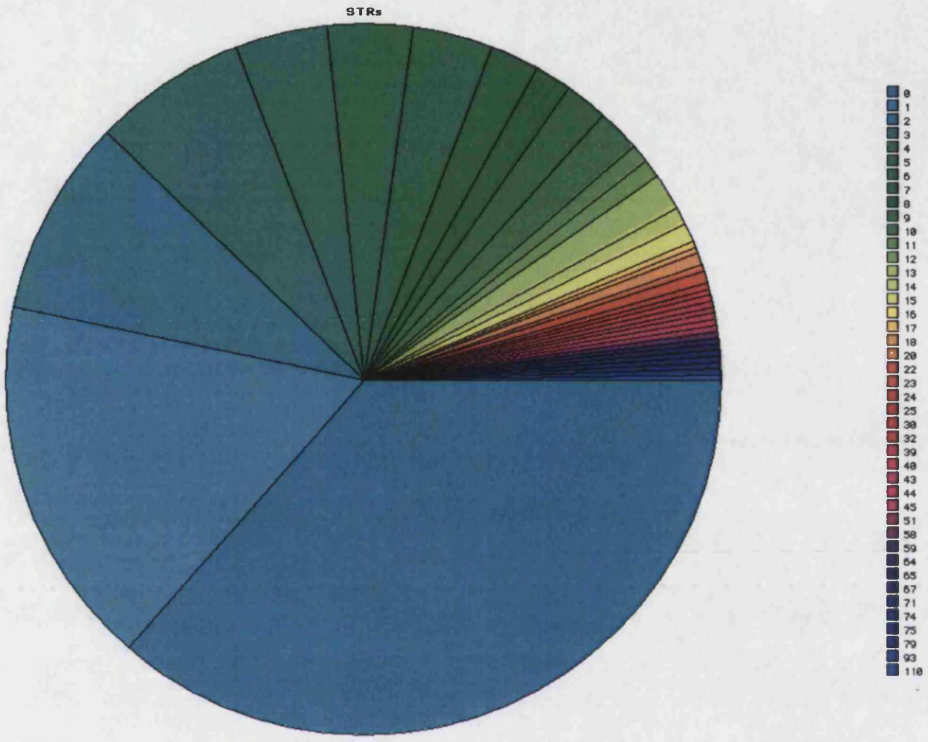


Figure 5.5: Asymmetric distribution of STRs in aggregated categories

It has to be made clear that the actual numbers of how many branches are in each category are not made available for anonymisation 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 particular colour in the pie-chart for the respective percentage (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 STRs category**).

Similarly, as indicated from the pie-chart, we can see that **more than 50% of the branches** have one or less ***STRs*** throughout the whole history of AML in the bank. We can then continue to observe the following correlation: *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 total of STRs. This implies that the vast majority of STRs (as shown in the Figure 5.5 above) comes*

from less than 7~8% of the entire population of the branch-network!! Just how fast this increase in density occurs becomes evident from the following graphical representation in Figure 5.6 below, where STRs are grouped in categories of five (branches that have sent 0-5 STRs are displayed in the first column, etc).

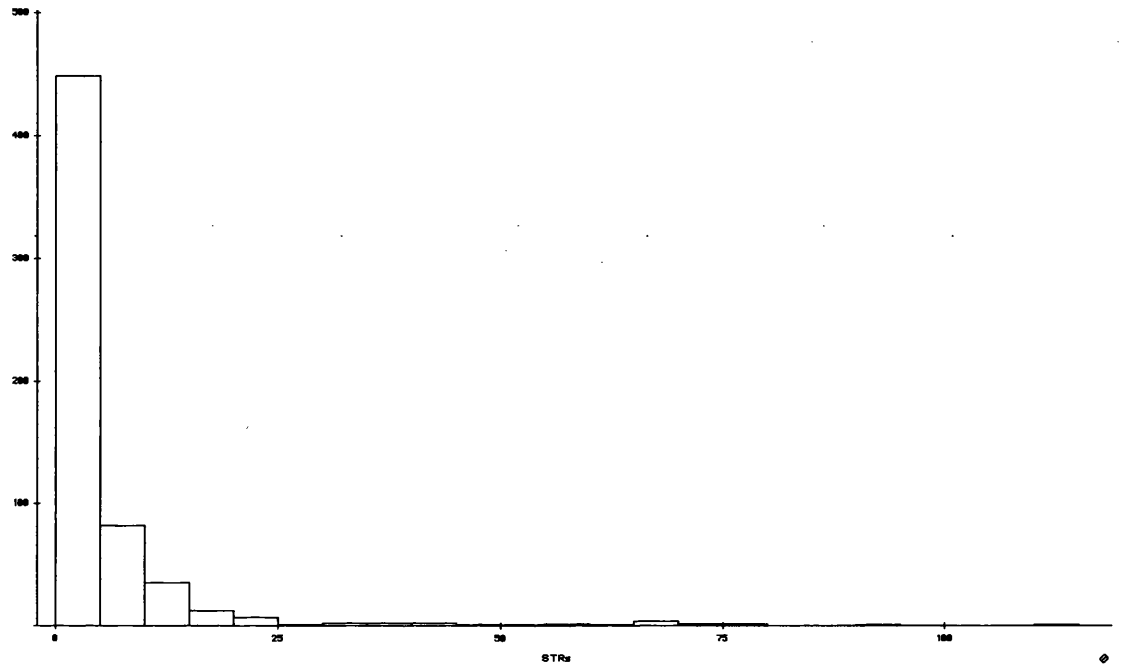


Figure 5.6: Decreasing STR-production graph

Different 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 of Greece. These branches are therefore typically 'ok' 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 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**[74]**...**We wouldn't be able to cope because of the massive volume and the backlog would be tremendous. As the Greek law has also become very strict after its renewal, reporting is going to sky-rocket and the employees are going to take few chances."

A testament to such a problematisation, and an additional fact to be considered is the effectiveness of the branches that are 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 manual and careful 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 of the bank. As this would be a cumbersome process, a small sample was selected of the *ten most active branches in reporting STRs to the MLAT* 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.

[74] Emphasis added

Figure 5.7. below indicates this percentage for the more active branches in reporting STRs:

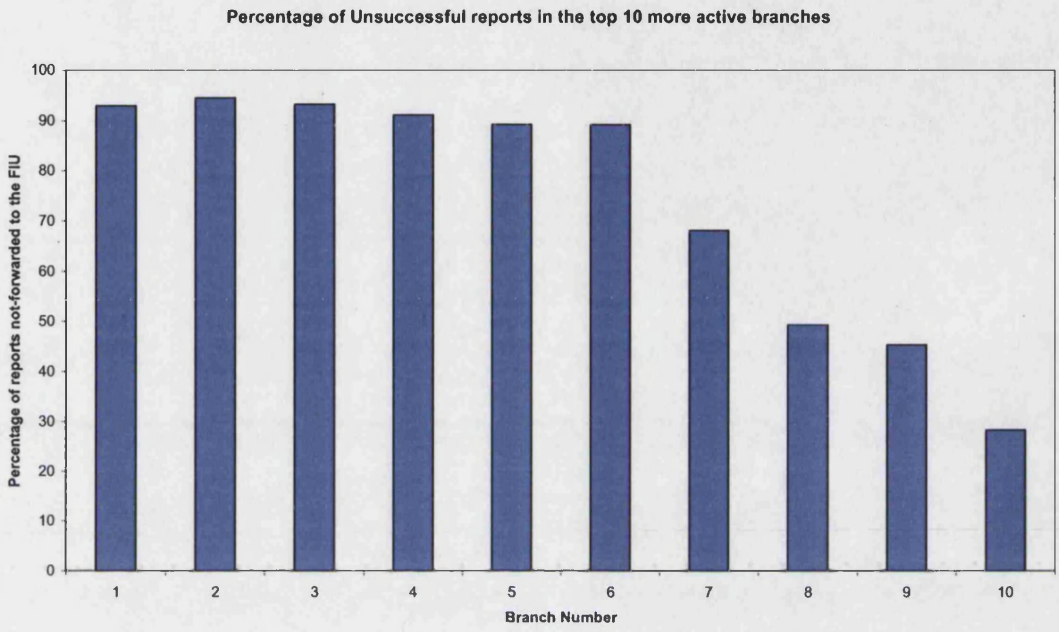


Figure 5.7. Top 10 most active branches in reporting
(percentages of unsuccessful reports)

From Figure 5.7 we can observe that amongst the top ten branches in reporting activity, the first 6 have a considerably high percentage of unsuccessful reports of around 90%. 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. 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% '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 STRs? 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[75] 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 dissertation set out to examine and one that would require considerably different methodological techniques.

Thus far the broader AML system of Greece, 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 technology within AML in Drosia Bank 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 – New Automated Solutions for AML

First of all it has to be made clear that unlike other countries, in Greece there has been no initiative whatsoever from the Central Bank or the Bank of Greece to urge the

[75] An 'Unsuccessful report' here means that after further analysis from the MLAT, it is not forwarded to the FIU. It is not connected to any other processes at this stage.

financial institutions towards implementing and adopting profiling or other AML-related technologies[xxx]. Every single financial institution acted on its own initiative, and therefore some variety can be observed in the Greek banking sector. Some financial institutions have already bought automated solutions, but most have built their own software for monitoring suspicious transactions.

Drosia Bank has had (as already discussed) a series of Information Systems, but never a centralised and bespoke system targeting particular aspects of money-laundering. Even though the focus of this dissertation 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, the latest system to be implemented in Drosia Bank.

As profiling technologies for AML were becoming fashionable around the world, and the software houses providing them truly successful in gaining disproportionate (to their efforts) financial gains, 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, etc), 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 by Drosia Bank as some monitoring problems of STRs needed to be looked at. Internet banking for example was not monitored at all for money-laundering or scrutinised 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 were 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 Drosia Bank included (without this list being exhaustive): Norkom, Unisys, Hughes Financial Analysis, Thompson Financial Services, SearchSpace, Intrasoft, 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."

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"

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 sub-systems 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 when the software is 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 realisation 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.

Following the decision to build the CHIMERA system in-house, and which is now operational in its first implementation stage, specifications 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 here 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 customised for Drosia Bank can only be updated by the Money-Laundering Analysis team. These three lists currently are: the CFSP[76] list from the European Union, the OFAC[77] list from the United States, and a complementary list from the Bank of Greece that basically forwards FATF requirements and countries that are sanctioned (currently only Myanmar at the time of that implementation).

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 the full consequences of a possible – and considerable – increase in the number of suspicious transaction reports. Profiling attempts, when they materialise, 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) The focus in CHIMERA is essentially to interlink with POSEIDON. Transactions that are being performed by tellers are constantly cross-checked for name verification against the CHIMERA system. In case the customer is

[76] http://ec.europa.eu/comm/external_relations/cfsp/sanctions/list/consol-list.htm
[77] http://www.ustreas.gov/offices/enforcement/ofac/

found in one of the suspicious lists then the transaction is automatically blocked and a chief-teller/manager has to be informed, and who then takes responsibility for further informing the MLAT of the incident.

4) It is useful here 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, and one that takes considerable amount of their time. This was discussed in relation to the opportunity that was given to allow 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. Staff within the MLAT also wanted the electronic submission to go ahead as some of the handwritten reports were so badly written by the tellers that it took quite some time to figure out what the report was about.

Following the design and implementation of CHIMERA, a few problems started to emerge that are worth discussing in brief. Some of them were emergent, and others were due to organisational problems and lack of sufficient coordination. Despite the fact that the initial feed into the CHIMERA system of database information for the suspicious transaction lists was done automatically from the CFSP and other lists, and that the format in which the lists were available was the Extensible Markup Language (XML[xxxi]), which is considered to be the most interoperable format available in computing, no provision whatsoever was made initially 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 the updates to the CHIMERA system would be minimal, even though done manually, was an underestimate, to say the least. 'Suspicious' lists always entail the possibility of sudden explosions (in scandals like the one with the government of Belarus) and the manual input of the names and details of all those involved became a cumbersome process that took considerable time away from some critical working tasks and investigations. Furthermore, shortly after the CHIMERA implementation, it was realised that the Case Management System (CMS), where STRs from the branch network are recorded, also required the input of the suspicious names from the widely available lists. Difficulties in the way the CMS functions, but also failure to address the issue of the interoperation between CHIMERA and the CMS, meant *not only that manual input from lists of suspicious persons and organisations* became unavoidable, but also that *this process of manually inputting was further* ***duplicated*** in order to update both the CMS and CHIMERA, hence doing the exact same working task twice.

This lack of interoperation between the CMS and CHIMERA exposes further the lost potential 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 Money-Laundering Analysis Team and the computerisation 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 however was never requested and an opportunity was missed for the integration and use of intelligence between the two systems (old and new).

But 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 reasoning is 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 are 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 can be minimized. Going through the CHIMERA manual, and discussing this issue with someone 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 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 the 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 realised, 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.

An additional problem that was realised in CHIMERA, insofar as it was interlinked with POSEIDON, was the matching of suspicious names provided in the lists of the EU, OFAC, etc, that are delivered in Latin-based characters, and with those kept within POSEIDON in Greek characters. An automatic routine was employed to convert the names from the Latin-characters to the Greek-characters within POSEIDON. A sample is provided below:

A → A
B → B
C → K
D → Δ
...

It was soon realised 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, and by typing the last name in Greek, an employee from the MLAT found that there was no alert whatsoever in any of the transacting codes. It was immediately obvious that something had gone wrong in the conversion of the name, and that had Osama bin Laden transacted with the financial institution by electronic means, 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'. Phonetically then, 'D' in English that is equivalent with 'NT' in Greek would require the conversion D→ NT. The problem was quickly rectified for CHIMERA in this case and the conversion was re-run.

But 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

researcher'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 DEMETIS would have been 'NTEMETIΣ' whereas the spelling of my name in Greek would be 'ΔEMETHΣ'. Here we observe the following:

D can be both Δ *and* 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 their number. 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[78].

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.

[78] 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

The Electronic Updates System

As this chapter gradually concludes, right before some broader comments about the Drosia Bank are presented, and before we move on to the discussion, it is useful to note that a very important and interesting 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 various other AML-related news.

A system that is being 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 utilised. 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 read anything due to the time restrictions that they face. 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 that have access both to the system to see whether their employees have been informed about the new information items, and to 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.

Broader comments

Despite considerable delays in the improvement of the overall AML system in Greece, 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 in Drosia Bank saw the AML domain as a challenging, 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 (i.e. FIU). Some brief comments were made in the beginning of this chapter regarding the situation of the Greek AML system. This was intentional, so that the discussion of the findings does not become de-contextualised from the immediate regulatory context. 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 also 'helps' and supports the creation of an internal bureaucracy that is required to sustain the working processes.

In this regard, the dispersed Information Systems that have been examined here in detail create a truly complex fabric of electronically-processed influences on Anti-Money Laundering in the operations of the Bank. As already discussed through various examples that include POSEIDON, the Bank's Case Management System, and CHIMERA (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; they recoil from each other, challenge each other, permit or deny each other, are blind to each other.

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, demonstrate that variable degrees of analysis expose the interconnected problems in a different degree of granularity.

But this chapter finishes with the quotation that started it, the knowledge that what we have gained in discussing any knowledge-creating path cannot but include those things for which we remain ignorant. The only benefit that one can claim by such an examination is an increased confrontation with the systemic complexity of the case being examined; 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 final chapter that follows, these aspects are brought together and the systemic complexity eventually confronted in the combination of systems theory as outlined in Chapter IV, and further expanded in the analysis, and in the multiple 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 were systemically expanded, while providing theoretical contributions in ST and practical contributions for AML.

"Εν οίδα, ότι ουδέν οίδα" [79]
Σωκράτης

Chapter VI: Analysis & Discussion

Chapter Structure

This final chapter deals with the analysis of the findings through the lens of systems theory by providing a theoretical synthesis that places AML and the case material of the previous Chapter V within the context of systems theoretical concepts as outlined in Chapter IV. A theoretical treatise is developed that constructs the Anti-Money Laundering domain as a system. Then the role of technology in the AML system is reflected upon (on the basis of empirical data collected and theoretical insights), thus dealing with the two research questions outlined in the very beginning of this dissertation. Following this treatise, theoretical contributions to Systems Theory are outlined and practical contributions to AML are further discussed. Finally, some conclusions are discussed, and considerations for further research are provided.

Introduction

The remainder of this dissertation must confront a considerable difficulty. Within the scope of analysis and discussion that will be carried out in this chapter, an attempt is made to synthesize the two distinct poles that have been presented thus far, and thence to bring together the core theoretical aspects of *Systems Theory* and the more practical aspects that have been outlined for *Anti-Money Laundering*. Amidst attempts to provide such a synthesis, some opening remarks will hopefully be of use to the reader by providing a set of clarifications for the analysis itself.

[79] "All that I know is that I know nothing" (Socrates)

The scope with which the synthesis between anti-money laundering and systems theory will occur is separated into two distinct phases. Firstly, some broader comments are provided on how Anti-Money Laundering can be viewed as a *system* through *systems theory*, while elaborating on the differences between AML-representations from different stakeholders. This builds on previous work that attempted for a first time to merge systems theory with AML (Angell and Demetis 2005). Secondly, following this initial step, such a description is re-visited to provide a novel re-conceptualisation of the AML domain by positioning Anti-Money Laundering 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 empirical evidence gathered throughout the case study, *the role of Information Systems within the construction of Anti-Money Laundering* is discussed, a description that will on many occasions rest upon the systems theoretical concepts that have been outlined in Chapter IV and the empirical data presented in Chapter V. This will manifest itself in different ways, in the descriptions given of the role of technology in the construction of the suspicious transaction reporting system, the communication of suspicious transaction reports, and also, the risk-based approach that has been the latest step within the evolution of regulatory initiatives.

The System of AML

While the word *system* has been one of the most abused, misused and misunderstood words of the English vocabulary, and one that has been hijacked from its initial theoretical provinces to be used in either various disciplines or in everyday life, there is nothing vague in the word *system* within the context of *Systems Theory.* Chapter IV has already outlined both the epistemological foundations that give rise to the concept of the system, and the interrelated theoretical concepts that the ontological presupposition of a system propagates (i.e. boundary, environment, etc). 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. Nevertheless, such a systemic conditioning does not imply a change in the unit of analysis within research. Even though the unit of analysis within this dissertation 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 constitutive difference between system/environment; cause-and-effect relationships between systems and their environments are shattered by the forcefulness with which complexity replicates within systems and affects their environment.

Despite any differences amongst systems or subsystems, generalisations (and hence practical or theoretical contributions) generated with the help of systems theory exhibit increased cross-context and cross-system resilience. The abstract level of the systemic language itself and the foundations of systemic properties help to accommodate multiple specificities. In other words, one is allowed to be extremely specific in his or her descriptions regarding systemic properties while utilising an abstract vocabulary. There is nothing contradictory in that. Combinations of abstractions may cancel themselves out into creating specific descriptions that penetrate the heart of a problem domain.

All these systemic attributes imply that there is a considerable need to stray away from a tidy demarcation that is typically projected within the broader realm of Anti-Money Laundering. This demarcation projects a hierarchy of AML stakeholders that function according to well-specified rules, and where problems can be overcome by the specifying further rules. Within AML, such a projected hierarchical *modus operandi* is observed in various ways, although always implying a considerable degree of linearity. 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 organisations. These levels can be designated as follows: the local, the national, and the transnational.

Transnational organisations are responsible for norm-production, and hence are believed to be (and to a certain degree they are), 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 ML, regardless of what possibilities or mechanisms these transnational organisations control for the diffusion of such momentum and the monitoring of measures' effectiveness. Examples of norm-producing institutions for

Anti-Money Laundering range from the United Nations, to the Financial Action Task Force, the Basel Committee on Banking Supervision, the International Monetary Fund, etc. 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 an uninformed value-judgment that has merely been institutionalised 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? Even more importantly, to what degree do processes exist that counteract such a top-to-bottom demarcation of control, and do they create additional difficulties for the AML itself? We will see in due course how such processes come into being.

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

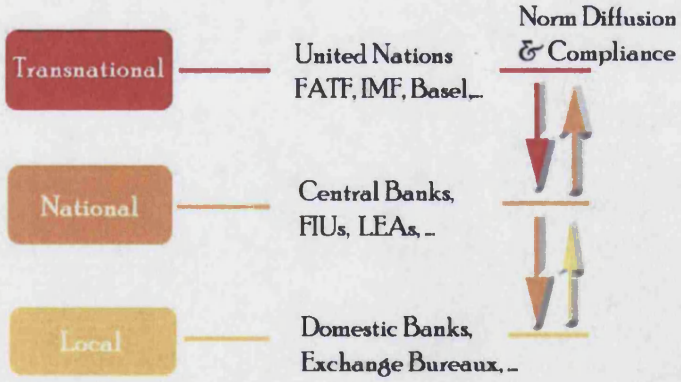


Figure 6.1, The Standard Model of the 3-tier hierarchy

Such tidy hierarchical thinking of the broader Anti-Money Laundering domain is clearly an oversimplification of the complexity that resides within the domain itself. Recognition of such a complexity, which – to a certain degree – becomes irresistible due to the large number of stakeholders involved in the domain itself, creates the need for moving away from such a linear method of differentiating between AML-levels and moving towards a systemic description of their influences. This implies a considerable 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 have little or no planned effects on AML itself. The idea therefore behind the three-level hierarchy constituted by transnational, national and local stakeholders needs to be completely shattered. Similarly, the idea of norm-diffusion in the linear sense needs to be abandoned.

Systems cannot be described by such attributes. Levels become inappropriate. This means that the AML-system cannot be characterised as the totality of the local, national and transnational stakeholders. However, via the description of the systems theoretical lens, the *system of AML* can be characterised as a complex array of subsystems (systems in themselves) that become prone to both positive and negative feedback exchanges between themselves, and that simultaneously oscillate the AML-system in different ways from a virtually non-existent equilibrium/reference state. Clear separation of these processes is impossible no matter what observer is utilised for identifying the AML system; for the unavoidability of systemic interpenetration cannot otherwise be accounted for.

The convenient myth that there is such a thing as an equilibrium state implies an observer that can observe the *systemic totality of AML* without carrying out a single differentiation, and such an observer does not exist. One can only study the domain itself by carrying out an internal differentiation, hence automatically creating a distinction between what can be studied and what cannot; what can be observed, and what by necessity is left unobserved. By treating the stakeholders (say a financial institution) as systems, one needs to escape the edifice that is mere compliance of well-structured and formulated rules, and move towards an examination of the underlying processes and mechanisms that feed the complexity of the system itself. Systems then become 'islands of reduced complexity' as analysed in Chapter III; the reduction is

necessary for observation to proceed, but that does not mean that there is a disregard for the complexity within the system. Quite the contrary; identification of internal processes (whether supported by technology or not) 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 collapses and gives rise to a loose assembly of institutional sub-systems, which are intended, through 'coordinated' activities (but never controlled activities in the causal sense), to combat the phenomenon of money-laundering. The regulatory belief that these systems co-align to target money-laundering also collapses as an oversimplification that undermines the intrinsic systemic complexities within such systems. In this manner, and if we take a single organisation as an example (say a financial institution or any other AML stakeholder along with the environment within which that institution operates), another need comes into being: the need to '*differentiate between organisations themselves (i.e. FATF, a Central Bank, a Domestic Bank) and the systems that emerge from the way these organisations 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). "A system is what it becomes, and not what it was intended to be." (Angell 2000) Beyond the organisational aspects, if one considers the *system* of technology, which surpasses the mere technical domain of its installation, things become much more complicated as demonstrated by the variety of information systems and processes of AML 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 considerable multiplicity of other systems with which it co-evolves. AML itself is structurally coupled with ML in a form of co-evolution that brings the entire co-evolving structure (AML and ML) within the realm of self-reference, and beyond the conventional ethical domain of good and evil. Furthermore, any assumption that there is a unity of purpose behind any such system implies a cause-and-effect process in controlling the outcomes, and that needs to be rejected. This means that *by adopting the systemic way of thinking,* the common justification for the existence of AML that ML as a problem *per se* is bypassed by the systemic necessity of

the system/environment difference, which points to the fact that one cannot exist without the other. Analytical differentiation, which is a prerequisite for observation, becomes an ontological coupling between AML and ML whereby their existences depend on each other. 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*[xxxii]. This is often because sub-systems 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 the outcome of their decision-making activities generates unexpected positive feedback. Such positive feedback tends to destabilise the working processes of another stakeholder within the AML System 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[80]), as well as compliance-fear and financial fines, generated a positive feedback that left the FIU of the UK (the National Criminal Intelligence Service[81]) in a state of denial, swamped with STRs and forced either to prioritise the reports or to put them on hold, unable to cope with their volume. There is a backlog of STR processing of more than 8 to 10 months between the time a suspicious event is triggered and when it is actually forwarded to a Law Enforcement Agency (LEA)[82], which is characteristic of the explosive complexity that can be witnessed, and one can only begin to imagine the organisational implications of such deficiencies (KPMG 2003).

Systemic considerations of such processes are therefore never straightforward. Such processes of interactivity, interdependence and co-evolution, exhibit a simultaneity of existence at various subsystems. As these subsystems interact in both structured and unstructured ways, their interaction generates emergent phenomena that can only

[80] 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 (mostly) technology considerably.
[81] NCIS – currently transformed as part of the Serious and Organised Crime Agency (SOCA)
[82] In the UK, a total of 500 staff work for the 57 LEAs (!) have to cope with the forwarded STRs.

become visible *a posteriori* the interaction. These complex interactions imply that the subsystems constantly interpenetrate each other.

As this constant interpenetration between systems, subsystems, etc, takes place, observers come along posing questions of the phenomena they observe within and between systems of interest. 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 (e.g. 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. 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 recognising 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 complementary recognition that *any function* (such as success or failure in 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 at this point, about the properties of the AML-system and how it may be described in general systemic terms, then a typical 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 organisations that exchange data. 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 are the properties of each such AML-system? What is its most

fundamental characteristic? 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 above, by turning to one of the most significant societal applications of systems theory: that of the functional differentiation of society, as described by Luhmann, a differentiation that does not, however, include technology in its account and influence. By seeking to outline and include this aspect, the aim is to extend Luhmann's theoretical description by positioning technology within such a schema, and thereby describing how technology comes to affect society, within both the realm of Anti-Money Laundering, and the scope of a broader stratum of systems where technology penetrates their functions in fundamental ways.

The functional differentiation of society & the role of AML

Anti-Money Laundering does not exist in a void; as already discussed, it is structurally coupled with money-laundering in a multitude of ways, and the two co-evolve in ways that surpass both conventional descriptions of cause-and-effect, and its implied linearity. But there is another important and complementary aspect for describing the way in which AML becomes co-dependent with other societal systems, while preserving its own hypostasis. 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 utilising their own elements.

The functional differentiation of society into subsystems is informed by four essential assumptions:

i) there are *functions* that characterise the subsystems in themselves, and these functions become constitutive of a subsystem's 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.

ii) The system of *society* is considered to be – within the systems theoretical approach for social sciences[83] – 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* that is central for any societal aspect.

iii) *Differentiations* within society are those that give rise to the constitution of subsystems within it. Such subsystems also communicate in the societal sense, as this is the primary function of the society within which they are embedded. The importance of communication is intertwined with the existence of the subsystems upon which the system is operatively dependent. 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 self-destructive mechanism indicates that subsystems within society also equip themselves with *additional forms, norms and codes* of communication that become an intrinsic and representative characteristic of their own functioning. In this sense, communication itself becomes differentiated within the formation of subsystems, and two modes of communication can now be realised. One mode of communication is used within the subsystem and is utilised to communicate the function of the subsystem amongst its own stakeholders (other systems in themselves), and the other that allows the exchange of communication – and hence codes – between different subsystems of society like the political, the legal, or the economic.

iv) Following functions, society and differentiation, *autopoiesis* becomes one of the most important characteristics within the functional differentiation of society into subsystems, for without autopoiesis the subsystems lose their

[83] As outlined in 'Social Systems' by Niklas Luhmann

> 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 above 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 2000).

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 – at its initial stage – 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 characterised 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 dissertation 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[84]? To attempt to resolve such issues within the systemic realm for AML, this dissertation resorts to the crucial issue of *coding.* In order to do that, it is important to see the interrelationships between the domain of AML and the attributes outlined above for autopoietic systems (function, differentiation and autopoiesis itself).

In this regard, and within the systemic scope of the functional differentiation of society, the *system of AML* can only be characterised as a system within the specificity of the aforementioned attributes, and hence an elaboration of those becomes necessary. Once again, how one carries out such a differentiation implies an observer-relative positioning, and ultimately remains an act of choice. This is very much true for any system, but one must not go as far as to question the ontological hypostasis of systems. It needs to be emphasised that such an ontological positioning is clear; systems exist. The epistemological consequences, however, are another matter. The aspects that determine 'how we know what we know' regarding systems and their functioning become substantially imposed by the observations and differentiations selected. Therefore, the issue of how AML as a system gains its hypostasis is a different matter from how it can be analysed and researched. 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 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). Following *functional systemic communications and interactions between these subsystems,* what **emerges** can be described as the perceived single entity that we may call the *AML system.* Even though schematically oversimplified in Figure 6.2 below (as is the case with any graphical representation), this description of the AML system strays away from the hierarchical mode of functioning depicted in Figure 6.1.

[84] A first attempt to examine the systemic nature of technology was presented at the end of the Systems Theory Chapter where organisations and technology were described as a self-referential and co-evolving structures.

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. It is this communication then that becomes responsible for the emergence of new 'structures'.

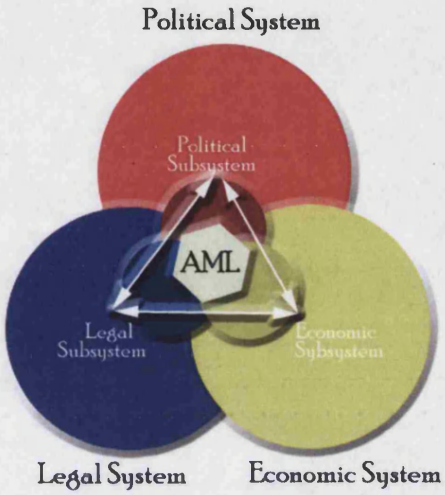


Figure 6.2: The functional differentiation of AML

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 the above graphical representation (a graph that again oversimplifies the issue) refer to the constitution of subsystems within the political, the legal, and the economic system. These subsystems express - by inter-communication - the systemic formation, constitution, representation, and sustainability of the AML system. The realisation of exploitation of the economic system had to be realised first of course – in what would become known as money laundering – along with its societal consequences, before political power and legislation were introduced.

Such a functional differentiation implies that diffusion of norms is not following a hierarchical mode of organisation. Every system contributes in a different manner within the broader schema of the emergent AML system.

The political system expresses the initial momentum within the function that characterises the political system itself, that of power[xxxiii]. The legal system contributes within its own function by constituting the illegality of particular acts and embedding within its system the expressions that can be further communicated for characterising the ontological status of money-laundering *within the legal system itself* (ontologies can be drawn differently, and hence that does not mean that the legal system defines money-laundering; this is merely a delusion that will become more evident later on). Finally, the economic system contributes by providing those organisational structures where the applicability of AML laws and regulations can be realised and implemented (financial institutions for example). Subsystems – at this level – indicate the unavoidable observation that not all of the political system is exercising its power for AML purposes; not all of legal codes refer to AML, and not all of economic functions are subjected to compliance with AML regulations. 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 reorganise for the production of a change that may occur accidentally or in an unplanned fashion (triggered by the environment for instance ~ ML in this occasion), or planned by the AML system that communicates its deficiencies to itself within its own self-reference, and subsequently, automatically to all other systems (political, legal, economic) within which AML exists. Through such a complex array of interactions and communications, it becomes clear that neither hierarchies nor control mechanisms are appropriate for a systemic description of AML. The idea that the *AML system* is something separate, which can be manipulated, is therefore completely shattered. 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 also; the relations they develop keep being negotiated systemically and it is this re-negotiation that contributes considerably to the self-referential evolution of the AML system itself.

This emergence of the wider international AML system from the functional differentiation of society and the major function-systems that dominate it is something that was previously described to be self-referential. This deserves some further consideration even though the description of self-referentiality has been provided in Chapter IV. Now that the dissertation has incorporated the functional differentiation of society within the domain of systems theory in order to analyse the AML system as a system in its own right, the issue of how self-reference participates in this can be better articulated.

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 that has been examined, it is such a subsystemic constitution that results ultimately in the emergence of an AML system. This tremendous systemic capacity of self-reference implies that an emergent system (e.g. 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 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 characterises them serves the function of generating autopoiesis out of autopoiesis when relating to systemic formation!***

This autopoietic transcendence from systems to systems 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 when other function-systems like the political, legal and the economic contribute in the process of differentiation. 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, as the property of autopoiesis would have to be complemented with a *function* 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-organisation and the re-arrangement of a system's elements and relations. However, beyond the concept of autopoiesis, it is the concept of *function* that represents a co-alignment of purpose at the subsystemic level, a purpose that is simultaneously expressed at the level where these subsystems are included (i.e. system). 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 realisation that within systemic formation (like the formation of the AML system), function, differentiation, and autopoiesis are equally necessary for the system's existence and operative closure. They are created together. And in this event, as with any other system that comes into existence, there is something more that brings and holds together all three primary concepts (function, differentiation, autopoiesis). That something is what we designate the ***code*** of the system that is being differentiated.

Coding

The issue of coding and the *code* that characterises a system lies at the core of this chapter. It will serve as a step towards combining systems theory, the formation of AML, and its systemic relationship with technology. 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 communicate the function of the system amongst its subsystems, 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 IV). 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, and 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 being systemically used in order to communicate the system's goals throughout all of its subsystems and as a reference point to itself.* This means that whatever subsystems may exist within the - functionally differentiated from society in general – 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 legal system 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 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 is foundational in system formations that are functionally-differentiated from society. As the code in itself characterises the primary

function of differentiation of the system, 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 2000). 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 the table below (Moeller 2006)[85]:

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

Figure 6.3. Codes and Systems: Fundamental unities of distinction

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 recognising 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

[85] This is an adapted version of the table presented here in order to indicate only *system* and *code*

> 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)

This makes the point of the primacy of a code for a function-system even more crucial. The code is not only a necessary paradox that cannot resolve itself (in being utilised by the system that incorporates it), but also a foundational aspect of the constitution of any system of knowledge and all action. Without this necessary initial asymmetry exposed by the fact that the code cannot be defined by the system, an asymmetry that takes the form of a paradox, the system would not have been able to expand itself or even communicate within its internal differentiations. 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 pre-requisite for self-reference.*

The very fact that asymmetry is a foundational prerequisite for self-reference places asymmetry at the very core of scientific evolution, and even more so, approximation, as an unavoidable consequence of this asymmetry. Without acceptance of such an asymmetry, self-reference cannot sustain itself, and collapses into a tautology. The whole scientific system would then become a series of tautological definitions that would escape application. But the moment an application takes place it implies a differentiation between *what is being applied,* and *what 'hosts' the imposition of the application.* That difference in itself is enough to form the basis upon which self-reference can expand through new operations (and always through new asymmetries and approximations). Asymmetries therefore become a necessary prerequisite for sustaining 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 functionally differentiates itself from other systems in society by referring to its code (legal/non-legal). Systemic interpenetration requires that the legal system influences other functionally-differentiated systems of society (such as the economy) 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, etc.

But even within the legal system, the code serves as a mode of communication between subsystems of the system itself. If we take the legal system as a whole then it becomes obvious that the subsystems within it also utilise the code legal/non-legal, as a means of both establishing and perceiving themselves as subsystems of the legal system (say a law firm). In this way subsystems become autopoietic, and they also gain the means of communicating with other subsystems within the system. The code of any system therefore plays a critical role. Regardless of how one may carry out internal differentiations within the legal system and hence attempt different subsystemic observations and interactions, the code remains primary to the concept of system and of any 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 of the system itself.*

The code of the AML system

Making the utterance that there is such a thing as an 'AML system' and that that system is a *system* as outlined in the foundations of the systems theoretical aspects presented in Chapter IV and expanded here in the analysis, means that the *AML system* displays all of the attributes discussed in Chapter IV (such as self-reference, emergence, complexity, entropic and negentropic effects, etc), 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 function, differentiate 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 discovering how that code is applied within the system, thus creating its function, and in effect, the identity of the system. As Luhmann notes in his book on Risk 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 organises 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 observation, 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, and hence it becomes evident that for the AML system, the *code is the unity of the distinction between suspicious/non-suspicious.* 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 functionally 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. As a fundamental code

for the system (system and code are structurally coupled), it provides – along with differentiation and autopoiesis – the function of targeting money-laundering.

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 no foundational value establishing what is suspicious/non-suspicious, there are only operations (ibid). 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. They have to signal to other subsystems, and to the environment of the system to which they belong, that suspicious behaviour is communicated. In fact, as this is the required function of all AML subsystems, suspicion is established regardless of whether there is an underlying process to support its validity. What is difficult therefore is abandoning the other side of the distinction embodied in the code (/non-suspicious). 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?

At the philosophical level, 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 re-instate 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 considerably influenced by the different organisational structures and managerial circumstances within which AML individuals operate. These processes are

also considerably influenced by technology and the complex informational processes 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 the monitoring of transactions, where a particular staff-member of a financial institution identifies as suspicious a single transaction (or series of transactions related to each other). The method for communicating such a 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-realise 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 create operations that will refer 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 (e.g. through particular typologies), the code suspicious/non-suspicious becomes constructed in its own right 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 (e.g. the legal system defines what processes are to take place and how ML should be handled), the variety of these processes and the complexity that their interactions recreate, become more impenetrable as their effects deepen. However, it is only the legal system, and in fact, the prosecution of an individual or networks of individuals that can determine whether an act can be classified as money-laundering (if individuals are eventually 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. Accepting that risk is always implied in the construction of the distinction between the terms 'suspicious' and 'non-suspicious', we can then 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 therefore, were being forced into re-realising 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 re-considered; 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 categorised, even when the perception of risk is communicated; its re-genesis will transcend any system that attempts to manipulate it.

For a theoretical treatise on self-reference and risk as well as practical considerations please refer to:
Appendix I: *A treatise of the Risk-Based Approach with practical considerations*

The role of technology in the AML system

Before the role of technology is examined within the AML system along the lines described above, and on the basis of the empirical data collected within the scope of the case study in Drosia Bank, 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 arisen 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 assume the incorporation of technology within the FIU itself, and the consequences of utilising different information systems for coping with the work in the FIU. The other 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 Greek FIU (see below).

One set of consequences has become evident in Chapter V of the case study through the in-depth study and description of a variety of scenarios within which technology places itself and influences AML work within a financial institution. 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 in Greece, 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 in Greece 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 dissertation. This work was carried out in order to support further the argument that technology is a system in its own right, both within the domain of AML that incorporates it, as well as in any other domain that is technologically supported.

In considering technology as a system within the realm of this structural yet constitutional differentiation 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, and the political 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? The answer to this question is no.

Technology resists much of its subordination to a collapsed *form* of application in a multitude of ways, mostly 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 and control of technology by individuals and organisations that adopt technology for application in a particular problem domain. Contrary to *form,* the concept of *system,* when referring to technology, implies that technology retains all of its systemic attributes *regardless of the problem domain that it might be structurally coupled with,* and that the influence that technology has in any problem domain lies in retaining this systemic character. Therefore, to see technology as system in its own right, differentiates the role that technology comes to play within any given problem domain.

Furthermore, the question becomes different within the tradition of second order cybernetics employed within this dissertation (mostly by referring to the works of Niklas Luhmann). What is the observing system that is able to differentiate between *form* and *system* insofar as technology is related to the observation being made? What makes current beliefs mostly reduce this differentiation regarding technology as *form,* and what is to be gained in examining the underlying processes in restructuring this difference?

In order to remain true to the core principles of second order cybernetics, the issues of observation and system (whether a function-system or not) need to be treated as intrinsically related. The constitution of 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 coming 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.*

It is precisely at this point that this dissertation departs from Luhmann's perspective in order to expand the systemic treatise of social systems (like AML) by treating technology as a system in its own right, while examining their interplay. There is ample support for taking such a perspective following the implications studied in the empirical

data collected throughout the case study and presented in Chapter V. Theorizing about the systemic nature of technology (and complementing it with further data), this dissertation seeks a theoretical contribution at the level where technology systemically affects other functionally differentiated systems.

Despite the vast 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 properties that can be attributable to the systemic character 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[86], 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 that technology stimulates within modernity. The underlying assumptions behind functional simplification and closure imply that technology is subordinate to the initial reduction of complexity chosen by any one observer, while technology itself restricts its consequences and becomes devoid of observations. This does not agree with the theoretical stance developed in this dissertation, 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

[86] Indeed Niklas Luhmann has not extensively analysed technology but has focused instead on primary aspects around it.

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) over its evolution, and which differentiates thinking from a purely reductionist approach to constructing a 'cognition'. 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?

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 – to a large degree – impenetrable and that this is precisely what grants technology a systemic character that is much more complicated that the picture portrayed by Luhmann, whereby technology is merely a form that hosts other functional simplifications. 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, and 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 characterise as linear and automated would have been impossible. This is not to be taken as a patronising assertion, or indeed as a celebration of the superiority of human-kind. 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 per second) 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 characterised by all the systemic attributes put forward in Chapter IV 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 the form of any other code. It is an abstract distinction for which both sides to the distinction are necessary. It is also universally applied within the system of technology, as every technology has to incorporate both automation and non-automation. 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, and without which selection of automation and thereby the initial reduction of complexity would have been impossible.

As nothing can be considered in splendid isolation, technology too cannot be seen to be 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 technological artefacts come together (either wittingly by their designers or unwittingly by circumstances of systemic interpenetration and complexity), the process of reflecting upon the distinction between automation/non-automation becomes considerably more complicated, but illuminating nevertheless. In the case of Drosia Bank, this process is considerably revealed by the exposition of the POSEIDON information system that still is the most central information system in day-to-day operations.

As 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 categorised 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 organisation itself in its use of this important information system for transacting, marketing, and other purposes. In this example, analysed fully in Chapter V, 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; as well as continuous interactions by staff members with POSEIDON that fed the system with multiple unique-identifiers of customers and wrong typologies.

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 centralisation 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. Within the realm of the new technology coming 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 re-constructed 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 the system!

From a purely operational perspective, none of this affected the customers of the financial institution itself, 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, investigating customers' total financial positions and transactions, etc. On a number of occasions, time consuming AML investigations thus became even more problematic; something that led to the utilisation

of other information systems (like the FTEM analysed in Chapter V). 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 case study, it becomes evident that functional simplification and closure remain insufficient for capturing the systemic dynamics that technology brings into play. 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 the image below:

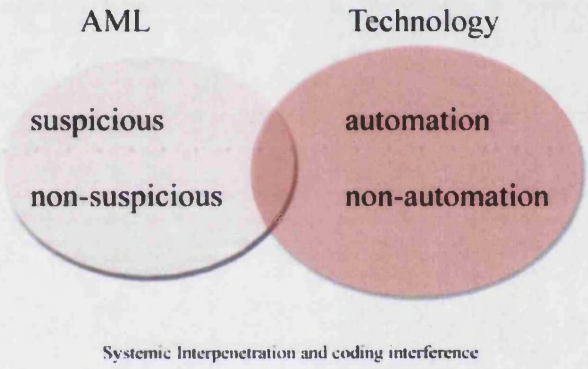


Figure 6.4. Interpenetration between the systems of AML and technology

The consequences in such a systemic interpenetration become evident on the basis of the two unities of distinctions that are framed for each system respectively. For the Anti-Money Laundering system, the major distinction that is communicated is the distinction between suspicious/non-suspicious, while for the system of technology this distinction captures the difference between automation/non-automation. Systemically, linear analogies here should be avoided. This means that a direct relationship between what is technologically automated and utilised by the AML system, does not immediately relate to suspicion. The same analogy can be drawn between non-suspicion and non-automation. Such an analogy would imply that the interpenetration between the two domains does not follow a direct correspondence or any causal pattern. 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.

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, BoG, etc, 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, 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 realised that the Case Management System (CMS), 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[87]. 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.

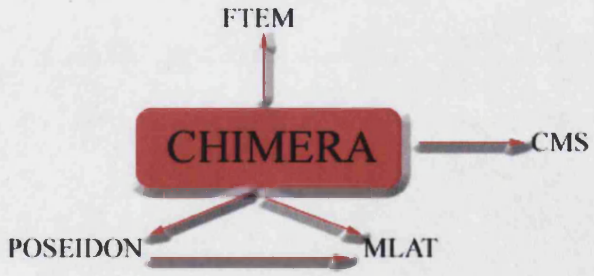


Figure. 6.5 CHIMERA influences

[87] The practice of blacklisting individuals particularly for Terrorist-Financing 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.

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 creates and 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. The example for that bank in experiencing such an increase is portrayed again below in Figure 6.6 that was constructed for the purposes of Chapter V, and put forward here again to make another important connection regarding the increase of STRs.

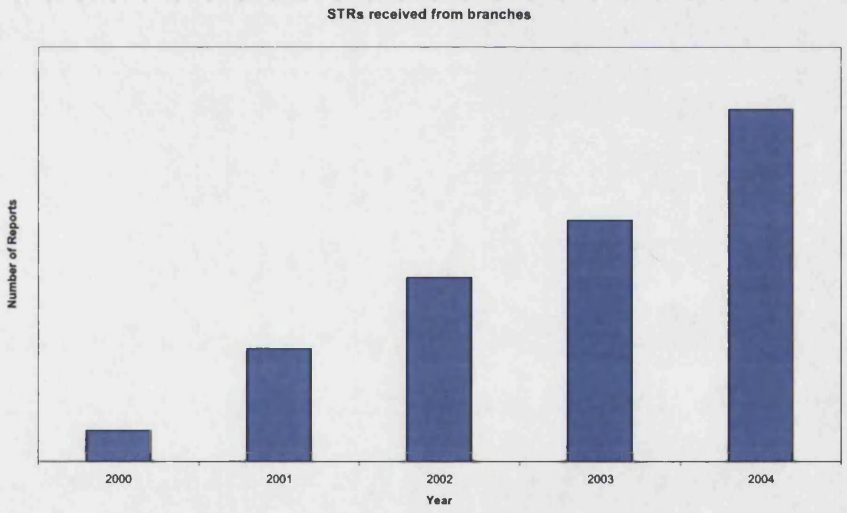


Figure 6.6.: STR increase in Drosia Bank

Beyond the increased vigilance and training that staff members in Drosia Bank have had, one cannot but include technology as systemically organising the increase of suspicious transaction reports for a number of reasons (within this individual financial institution). The CHIMERA system was explicitly designed for such a purpose and integrated within POSEIDON. But 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 financial institution 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.

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 dissertation, 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 Greek Banking sector? Has the number of STRs increased overall at the receiving end (the Greek FIU), and if yes, what has 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:

a. Aggregate data on the *total number of STRs* received by the Greek 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.

b. Aggregate data on the *total number of prosecutions* for ML per year

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, the data for this period remain representative of the Greek AML system.

Below, figure 6.7 presents the consolidation of these two sources that were disclosed to me during my research. The blue column represents the number of disclosures to the Greek FIU in the form of STRs, while the purple column represents the number of prosecutions for each corresponding year. The horizontal axis refers to the particular years for which data were provided.

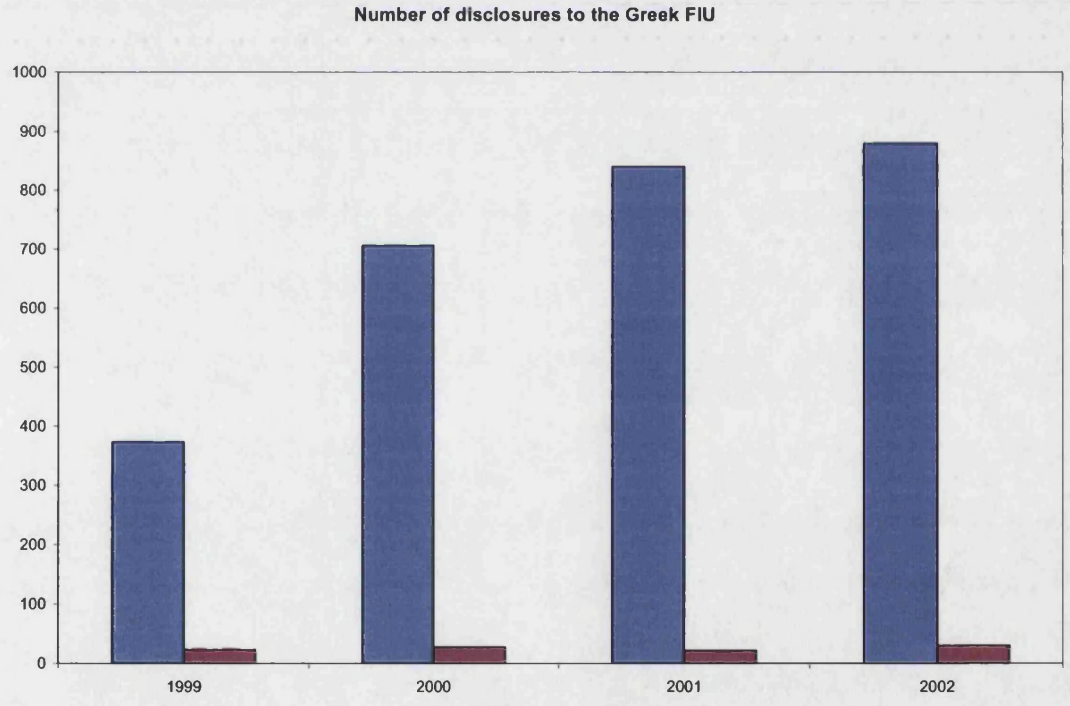


Figure. 6.7 – Disclosures/Prosecutions for the Greek AML system

One cannot but observe in this figure 6.7 that while the number of suspicious transaction reports was nearly doubling over the period of 4 years, 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 the Chapter IV, namely the concept of systems as 'islands of reduced complexity'. In order to evoke this concept, and to apply it in the particular circumstance, we require a differentiation between two further systems within the totality of the AML system. Having previously established that 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', and the only consideration to be made analytically would be how the complexity of one system feeds forward to the complexity of 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 an underlying stratum of technological implementations, the system of ML-prosecutions unavoidably rests on manual processes. In effect, the system of ML-prosecutions can be characterised 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 (e.g. 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, and this activation impacts on how STRs are being generated within individual financial

institutions, 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 utilising the distinction between automation/non-automation, affects the proper function of 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. As an 'island of reduced complexity' itself, and even further, one facing a double-reduction in complexity, the system of ML-prosecutions faces an ever 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![88]). 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 researcher found it at very least ironic that some FIUs (e.g. AUSTRAC[89]) proudly proclaim an increase in the volume of STRs as if such an increase in itself constitutes a measure of the effectiveness of the national AML system. It is interesting here to note that in Australia, 10.7million STRs in the year 2005 led to 1,743 investigations, a mere percentage of 0.016% 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[90].

Exploring this dynamic behind the interaction of generated STRs and prosecutions raises the potential of theorizing further on the systemic nature of both technology and its interaction with AML, as well as regarding AML as a system in itself. This first points towards the aspect – through observation – that the designation of an entity like

[88] Reduction of complexity in one system may of course trigger an increase in the complexity of another as in this case.
[89] The Australian FIU even congratulated the UK FIU (former NCIS, now SOCA) upon an increase in the number of STRs received year after year.
[90] http://www.fsa.go.jp/en/index.html

'the totality of the AML system' becomes paradoxical for analytic purposes. The somewhat fashionable and recent term that the world of AML has adopted, that of a 'holistic' approach in AML, is therefore misguided; the 'total' 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 generalise 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 Greece and the number of prosecutions, it becomes evident that the description developed in Chapter IV, 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'. Technology reconstructs the methods for the reduction of complexity through automation/non-automation, and has considerable effects on other systems with which it becomes coupled. 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 (like in the aforementioned example between the systems of generating AML-cases and AML-prosecutions) 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 a problem domain like AML, comes to reduce the complexity of the system that it is supposed to counteract (like ML through profiling software, data mining platforms, behavioural modelling exercises, etc) simply by automating aspects of ML (and of course, automatically leaving some other aspects non-automated). This however must not in any way be taken as a causal mechanism; the delusion of linearity at the level of technology creates a multitude of

complexities for the system of AML, regardless of the subsystems that one may designate. This implies that a necessary reduction of complexity in one subsystem may lead to an increase of complexity in another subsystem within the broader system examined.

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 in what is known as the *social construction of reality* (Searle 1995). This practically implies that humankind and organising societies come to refer to a reality (the environment of their system) that is socially constructed, and is rendered into reality by interaction between systems and their environments. In this section, it is argued – following from the treatise of technology as a system in its own right – 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 generalising 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 money-laundering purposes).

Current Anti-Money Laundering practices generally place technological artefacts (be they combinations of software and/or hardware) 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 V and the instances of technology being used (POSEIDON, CHIMERA, Electronic Updates Systems, FTEM, Case Management System, etc), information systems can be classified into the following categories:

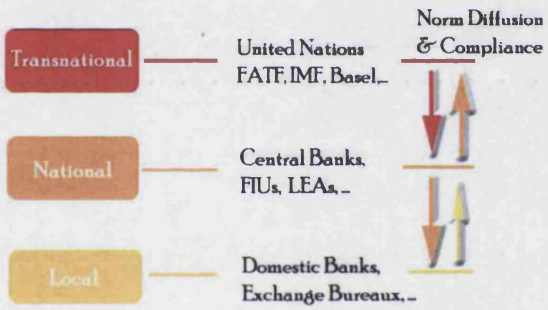
i. *Information Systems that target money-laundering explicitly* (such as the CHIMERA system) or used for AML purposes (such as the CMS in Drosia Bank). Such information systems are typically integrated within transacting systems of stakeholders that may be affected by money-laundering, and they aim at preventing ML taking place (e.g. 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.

ii. *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 considerable interdependencies that make it difficult to determine 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 interdependencies, technology therefore 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 I), 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.

Let us return for a moment to the image that was presented at the beginning of this chapter in order to indicate how perceptions of AML come to be constructed, and how technology enters the picture.



From a stakeholder operating at the Transnational level, say the European Commission, 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 (e.g. let's take the AML system here) 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.

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 dissertation. 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 (internally 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 specificity of suspicion. These subsystems can however be considered in relation to AML, insofar as they systemically affect the constitution of the problem domain and the construction of its suspicious/non-suspicious code.

In this manner, as it became evident within the scope of Chapter V 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, etc). 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. Every technological subsystem therefore – based on the fundamental premises of observation as developed previously – 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 realised, thereby defining what AML is for a stakeholder that has assimilated the technological subsystems within its own organisational structure. 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 re-organization of the systemic codes (those of technology and AML respectively), bottom-to-top processes that arise from complex interactions come to counteract top-to-bottom designations of how AML should function, or even how it is defined. In other words, technology and the myriad complex interactions it comes to engulf 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 – as amply demonstrated in Chapter V – 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, organisational structure, procedural resolutions of system/environment conflicts, and ultimately, operative closures. This complexity however 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 communicating suspicion by creating a temporal asymmetry between suspicion/non-suspicion (without the code being dissolved as previously analysed), but also its very existence serves the systemic function of cutting down on the underlying complexity for communication to be facilitated in a highly informationally-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 Law Enforcement Agencies 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 and not, there is a number of benefits to be considered in the broader AML system, which would also include the FIUs, so that feedback mechanisms would reduce the white noise in the hope of a more effective communication of suspicion. This is expanded further on the section below on 'Theoretical and Practical Contributions', but prior to that – and as a stepping stone towards this aspect - it is useful to consider the relationship between technology and human activity systems embedded in AML, and to extrapolate from that to develop a general systemic consideration.

From Bureaucracy to 'Electreaucracy'

In this section I would like to put forward a concept that attempts to encapsulate the technological problematization of systemic interferences that various technological artefacts have come to construct. The previous section described how information systems and human activity systems interfere with each other within the problem domain of AML. This interference at the level of the technological code (automation/non-automation) upon traditional organizational structures that depend on human activity systems, I call *'Electreaucracy'*.

A similar, although quite different idea named 'Cyberocracy' has been developed previously by Ronfeldt (1992). That concept can be seen as an aspect of the post-bureaucratic state, much as the information society was seen as an aspect of a post-industrial society. Furthermore, the concept was applied to indicate both major changes in the nature and conduct of government, and various sources of informational power that dominate government (ibid).

For bureaucracy, a concept analysed at length in organizational theory and diversity, Max Weber first contended that it was the organizational manifestation of the rational spirit. Accordingly, it was such an efficient and powerful means of controlling men and women that, once established, the momentum of bureaucratization was irreversible (Dimaggio and Powell 1991). Long before the concept was assigned a pejorative meaning, that of impeding progress and efficiency, Weber saw competition amongst capitalist firms in the marketplace as the major drive towards bureaucracy (ibid). Within the scope of the institutionalisation of the concept of bureaucracy, along came the negative meaning, and debates raged in organizational theory concerning structural differences and what form an organization should take to become more efficient within its bureaucratic precondition: loosely structured, unstructured, hybrid forms, and all sorts of mystically-structured organizations all suddenly made their appearance.

In what I term Electreaucracy, information acquires a double contingency. Information succumbs to a technological encapsulation that is based on the fundamental code of automation/non-automation, and at the same time information has to be communicated to traditional bureaucracies by means of interoperation. Bureaucracy and Electreaucracy

are then bound together by the transcendental property that is complexity. Regardless of the different operations that each entail, both in the bureaucratic order and within Electreaucracy, one can find processes of complexity that are structurally coupled; that is, processes whereby *the complexity within a Bureaucracy stimulates processes within Electreaucracy that affect the latter's efficiency and vice versa.*

Engineering and design disciplines have had a large impact in the rebalancing of these two sides. Bureaucracy was (and still is) seen as something that can be improved with the imposition of technology. This viewpoint implies that one can study how a bureaucracy operates, and subsequently incorporate (by design) a technology that automates part of that bureaucracy. This also implies the belief that technology is constructed on the basis of available information concerning the operative closure of the bureaucracy, and that information becomes somewhat subordinate to the function of the bureaucracy itself. Internal Complexity, however, is present in any structure; and Electraucracy implies just that.

Electreaucracy is essentially about the organisation of informational elements on the basis of the fundamental code of automation/non-automation. The consequences of such organising, in conjunction with more traditional bureaucracies come to create interesting yet often problematic dynamics. The delusion of easier manipulation of electronic information by technological means collapses when one looks more closely into how what is being manipulated within the realm of Electreaucracy comes to affect the bureaucracy in ways that often become highly contradictory. Complexity is hence seen as something that needs to be solved; not as something that is generated by stakeholders and by the means they employ in order to operate in any organisational structure.

In this respect, the example given previously in this chapter regarding a nearly static number of Greek prosecutions in respect to a continuous increase in STRs is characteristic of this problematization. While Electreaucracy operates in an electronic realm of large database systems, sophisticated manipulation of data, etc., a more traditional bureaucratic order is based on hierarchical management, and constructs its response to electreaucracy by means of optimization. The negative effects become

evident as volume becomes noise, noise generates complexity, and complexity is forcefully reduced by bureaucracy.

Theoretical and Practical Contributions

In this brief section my intention is to summarise some of the key theoretical and practical contributions of the dissertation.

When it comes to considering theoretical contributions, two criteria can potentially be used to examine their validity. One criterion would be the expansion of an existing theory in some well-identified manner. This theoretical expansion usually takes place with the help of empirical evidence that – by extrapolation – assists in generalised ideas that can be incorporated within the theory. The other criterion for a theoretical contribution involves the applicability of the theoretical ideas to a practical problem domain. Even though the latter case may appear to constitute a practical contribution, it primarily constitutes a theoretical contribution as it allows for the theory to be tested and applied within a potentially novel problem domain where the core of the ideas underpinning the theory have not been previously used for that purpose.

In respect of the first criterion for a theoretical contribution as portrayed above, it has been discussed that within Luhmann's theory of Social Systems there is a technological treatise that describes technology by means of functional simplification and closure. Devoid of general systemic properties on technology, Luhmann's theory fails to examine *technology as system*, and hence the systemic effects, which (a series of) technological artefacts may have upon a variety of problem domains, is underplayed by technology's perceived supportive role. Technology is hence seen as subordinate to other systems. In this dissertation I feel that the empirical evidence and the treatise provided outline a picture of complexity within the technological realm that exhibits all the systemic properties of interest (e.g. self-reference, code, autopoiesis). It then becomes evident that *technology as system* creates emergent phenomena that counteract top-to-bottom processes by other systems (e.g. the legal system). In countering such top-to-bottom processes, a more complex organisational structure emerges at the level

where information becomes treated in an automated manner. 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 considered (if any meaningful intervention is to take place). Technology is therefore recognised as a system in itself, and the effects of such a recognition involve an increase in complexity caused by technology and its systemic interference (and interpenetration) with other systems.

As for the second criterion concerning a theoretical contribution, the very application of systems theoretical ideas on the problem domain of Anti-Money Laundering constitutes a contribution in itself. 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. By treating the problem domain of AML at the core level of key ideas from Systems Theory I feel that an important goal has been achieved. 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.

In summarizing the key theoretical contributions outlined above, this dissertation has:

a. Provided a theoretical description for Systems Theory by taking the theory's core theoretical ideas and using them for a re-description of *technology* in the systemic sense. This has allowed for a description of *technology as system* by an examination of the systemic properties of code, function, autopoiesis and self-reference.

b. Applied Systems Theory to the domain of Anti-Money Laundering, thereby providing yet one more application domain where the versatile systems theoretical ideas can find fertile ground for further elaboration.

Regarding practical contributions, these refer to the problem domain of Anti-Money Laundering and target more pragmatic realisations that could lead to improvements in the domain itself. However, such improvements can only be realised in a self-referential manner, from the perspective of the system utilising them (otherwise the only meaningful relationship underpinning general effectiveness would be that between *the total number of submitted STRs to the number of prosecutions* – that relationship however has been analysed and shown to be arbitrary in itself, and hence no single measure can exist for monitoring their effectiveness). A few basic issues that can be considered as practical contributions are:

a. The consideration that each financial institution constitutes a complex AML-stakeholder, and an examination of AML working processes must be methodologically sound because a complex array of information systems interdependencies and manual processes for determining suspicion come into play. For the particular stakeholder studied in this dissertation (the case of Drosia Bank), a variety of information systems were examined and these had a much broader effect on the construction of suspicion than was originally expected. The internal effects of the increase in the volume of STRs that the bank has had to cope with, as well as the complexities underpinned by the POSEIDON system, constitute just two examples of what areas can be looked at in the deconstruction of an STR-system of a bank. Whether the same methodology can be applied to different financial institutions remains a question to be explored, but regardless of the results, in highly context-specific circumstances there are areas that can clearly be extrapolated and used to examine the conditions in other financial institutions. One such example is the extent of asymmetry in STR-generation throughout the branch-network of the financial institution studied. The same analysis of other financial institutions can be attempted, and potential reasons for any stark differences that may be uncovered can be examined more deeply (and further attempts made to

investigate qualitatively where these differences can be attributed). In this way, beyond the inexorable trend for the quantification of everything within AML (a condition often imposed by Central Banks that appear to be eager to see the 'whole' picture), financial institutions could undertake a qualitatively-based study, in order to strengthen areas where further improvement can be identified within their handling of AML-related issues. Integration of the risk-based approach may then become informed by both quantitative and qualitative techniques that not only derive from the institutional order (say regulatory guidelines), but also become customised at the level of the financial institution itself.

b. The practical relationship between technology and Anti-Money Laundering, as examined in this dissertation, re-creates the constructed associations between the two. Technology is not seen as a solution to the problem domain of Anti-Money Laundering, and is by no means reduced to what are broadly known as profiling technologies. Profiling technologies (such as Searchspace, Mantas, Norkom, etc.) are but a small technological subsystem that affects Anti-Money Laundering. These target the automation of suspicion and its algorithmic identification, while they 'contribute' towards a substantial increase in the number of STRs. Beyond such technologies, the central thesis of this dissertation revolves around a study of peripheral yet highly interdependent information systems that influence AML within a financial institution. Together with a number of working processes that are context-specific, these systems come to construct the dynamics of identifying suspicion. The interdependencies of various information systems within a financial institution, along with the managerial and operational issues raised in any business setting, demonstrate that there is a deeper link between technology and AML, and that this link should be considered very carefully. Within the modern realm of technology, a considerable irony comes into play. For within the domain of AML, technology, which constitutes the basis for automation and quantification, is utilised for the purpose of demonstrating compliance. When however, as the MLRO of Drosia Bank commented in an interview, we come to realise that 'Compliance is not quantifiable', we reach an interesting antithesis. Technology, which is the basis

for automation and quantification, is used for the purpose of demonstrating Compliance, while compliance in itself cannot be easily framed in these terms.

Epilogue

The function of an epilogue is often one that resembles truth in literary drama. Thus, it remains a delusional construct that projects the idea of closure, a concept that has been systemically fought throughout this dissertation. In this sense, the dissertation in itself can be looked upon as a system in its own right; a system with structure, organization, and conceptual elements that are exchanged for alternate interconnections, and hence, for the production for alternative interpretations. The system grows, re-constructs itself, and supposedly culminates with a few closing remarks; an epilogue that closes the loop and brings the system to an end. This however, strays considerably from the association that the author seeks to make with the concept of self-reference. A system can be further expanded; it can inform its environment if some (or all) of its elements are communicated to other observers; it can even seek to reconstruct conceptually a problem domain. If it fails in all of these tasks, the system dies.

Regardless of what evolutionary steps will be taken for the conceptual core presented throughout this dissertation, the distinctions have now been made. As Pinter remarks, 'a writer's life is a highly vulnerable, almost naked activity…the writer makes his choice and is stuck with it[91].'

The hope, however, that a theory of self-referential systems has been considerably elaborated on a pragmatic problem domain like AML, and has also been expanded to include technological effects, does remain the author's hope. What has become evident throughout this dissertation, and in particular through the presentation of the empirical findings, remains the underlying informational complexity, which is considerably more deep-seated than an application of a profiling technology. The first practical results as a consequence of this thinking are discussed in the Appendix as an example of the risk-based approach applied to a financial institution. Further research can expand on this

[91] http://nobelprize.org/nobel_prizes/literature/laureates/2005/pinter-lecture.html

theoretical and empirical agenda of deconstructing a suspicious transaction system of a financial institution. National or International implications can be further scrutinized within these dynamics.

Finally, all that the author of a dissertation requires of its creation is some degree of internal-validity. While the methodology has been laid out in some detail, and the author has attempted to integrate as many aspects as were of interest from the empirical data gathered, it remains inconclusive whether considerable variability in this research agenda would have been displayed by another observer, and ultimately, by another author.

The impossibility of such a possibility remains a paradox. One observer cannot create preconditions for the observations of another. What the author hopes of the reader is some degree of compassionate understanding and a recognition that the underlying *logical* mechanisms that gave rise to this construct, which we call dissertation, are equally self-referential. They are equally self-referential to the construct to which they give rise (the dissertation), and equally self-referential to the construct that the latter describes (AML & Technology). Logic therefore, and even more explicitly, the logic of the author behind the construction of this dissertation, remains a self-referential system.

Logic, serves the function of being able to justify itself, and hence in doing so remains inescapably intertwined with any entities it produces. In this regard, logic creates a distinction: the distinction between logic/illogic.

While the author retains the right to this asymmetry in the previous distinction, the author can only hope that the second-order observer, the reader of this dissertation, will have found the distinctions between logic/illogic, truth/error, consistency/non-consistency, considerably imbalanced and asymmetrical.

What side of each distinction has been chosen shall be left unexplored.

Appendix I:

A treatise of the Risk-Based Approach with practical considerations:

An informal account of the self-reference in the risk-based approach and an application to a financial institution in the UK

For the purposes of this Appendix, I will somewhat change the style of writing to a more informal one and attempt to describe the story of how this deep theoretical treatise and way of thinking has – almost as an emergent phenomenon – came to be applied for a first time in a financial institution in the UK, and has influenced my viewpoint regarding what is now known as the *risk-based approach.* This is more of a personal account, and acts a postscript at the same time.

The technique about which this Appendix is written, was conceived of almost accidentally while thinking in systems theoretical terms about a pragmatic problem that I had to resolve and/or explore. 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 story is told as vividly as possible.

In the year 2004 I started working at the London School of Economics as a research analyst for a European Commission project on AML entitled 'Spotlight'. 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 average in the industry was about 4% True Positive Rate, and thus for every one hundred suspicious transaction reports that was flagged by technology, only four came out being truly suspicious after careful manual examination and proper scrutiny. 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.

In dealing with the issue of attempting to model ML our team therefore requested some assistance from a financial institution that was a Spotlight partner at the time. We 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, etc. In fact, as far as I could see at the time, no consensus could even be made about what might even constitute a 'model', and resolution of the semantic problem was (and still remains) necessary. Three years down that line and I have come to the conclusion that semantic problems of this type are practically without a solution.

Nevertheless, research must go on. I remained in negotiations back in 2004 with the head of the money-laundering analysis team of the financial institution who was dealing with the issue of 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. There was a need to associate customers with substitute codes so that we could know what transactions corresponded to the same people. Thus, Gordon Brown for instance became SEC01363845, an unidentifiable alphanumerical combination for which however different transactions in different points in time could be linked.

The anonymization sequence 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 they were sent off at my office at LSE. A colleague still recalls the horror engrained in my face when I was faced with about 15 DVDs containing an approximate 250million financial transactions that were dispatched with a courier[92] service.

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.

[92] Fortunately, unlike the HM Revenue & Customs loss of 25million peoples' data (including National Insurance numbers, addresses, bank details, etc) our transactions were not lost (and had been anonymized for that event).

What does one do with 250million raw financial transactions when looking for suspicious ones?
My opinion was (and remains) that there are two distinct possibilities if one wants to analyse financial transactions for ML:

i. You have a model. 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.* That set is subsequently examined manually by staff members of the financial institution, and it is determined (case by case) what occurrences within the set are really worthy of submission to the FIU as potential ML-cases.

ii. You attempt to deconstruct, from financial transactions, *specific transacting patterns* that could potentially relate to suspicion. This deconstruction is not done by filtering out potentially suspicious transactions from non-suspicious by applying a model of some sort, but much rather as a bottom-to-top process. Data can potentially be data-mined and subsequently patterns of transaction 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. Financial institutions around the UK (those that we had access to at least, and others we've heard of) 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 ... These parameters were quite simple, and mostly had evolved around age, time of association with the financial institution, etc.

But let us go back to the problem. What does one do with 250million financial transactions? According to the two methods presented above, the first one would be impossible for our research project. It would mean that we would have to take precious time out 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 therefore. 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*'.

I started looking at the second possibility more closely, and differentiated the question slightly to accommodate the new possibility. How does one manipulate 250million 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 250million financial transactions on a 3-dimensional malleable plane that could be manipulated, rotated, parameterized, filtered, etc. I must say, it looked beautiful. 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 realise that complexity is a fundamental property of system, and that it can be further described as a transcendental property. Hence, transactional complexity turned into numerical complexity, numerical complexity into profiling and algorithmic complexity and the latter into visual complexity. No matter what form it took, complexity was present.

I went back to the last settled question: 'How does one manipulate 250million 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 known 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 functionally utilise 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 utilised, and further to consider the issue of 2nd order observation. It turned out that even though these two were intertwined, the latter step was much more apocalyptic in its exposure (and relation) to ML-modelling.

The distinction that was primarily utilised was that between the:

i. *STRs that were submitted by staff members of the financial institution, were found to be positively suspicious after manual analysis by the AML-team and were consequently submitted to SOCA (the UK FIU),*
ii. *STRs that were submitted by staff members but were found not 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 utilised 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, 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 VS automated True Positive Rates. For instance, whereas staff members performed very well, and typically around 50-60% 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 4-5%). All the difficulties created by the poor performance of technologically-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 as shown in figure A1 below.

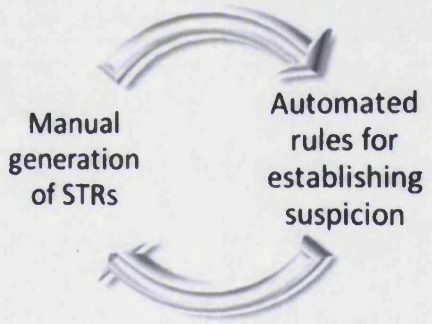


Figure A1. Feedback loop between manual generation of STRs and automated rules for establishing suspicion.

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 considerably. I then made the following differentiation:

i. 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.

ii. *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 and simulate and model ML.*

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 corresponding account numbers of customers that had already been reported to the FIU. These were in the reference form discussed previously, 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 positive provided that the model is used functionally to differentiate the transaction set and reduce the underlying complexity. Its specific function is to: *be applied to the totality of the available transaction set and act as a filter that isolates from the totality of the transactions that take place in the financial institution, only those raw transactions from a bank's transacting database systems 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.*

I describe the entire process in the steps below:

i. First, we may differentiate between staff reports that are further considered to be suspicious and those that are not. This is only possible after manual examination from ML-analysis teams examines each internal STR one-by-one, and determines whether further reporting to the respective FIU is necessary.

ii. 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.

iii. Various data fields are kept within the Case Management System for which a typical field would be the account number.

iv. 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'*

v. A query can then be performed to isolate from the raw transaction data of a certain period (say the past 3-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 iv), and where each line corresponds to an account number.

vi. 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.

vii. This new raw transaction dataset effectively holds information on the transacting patterns followed by money-launderers. Further discovery of such patterns and their isolation can be done through data-mining software that can isolate the aggregate typologies where launderers operate.

viii. The discovery of trends and the customisation 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 more than y-number of data-fields in their transaction databases, and only 10% of those data-fields appear to be important in ML-behaviour (for their own clientele and customer-base), then it makes sense that efforts around the selection of parameters, etc, would have to be appropriately customised.

The aforementioned steps are depicted in the following diagram:

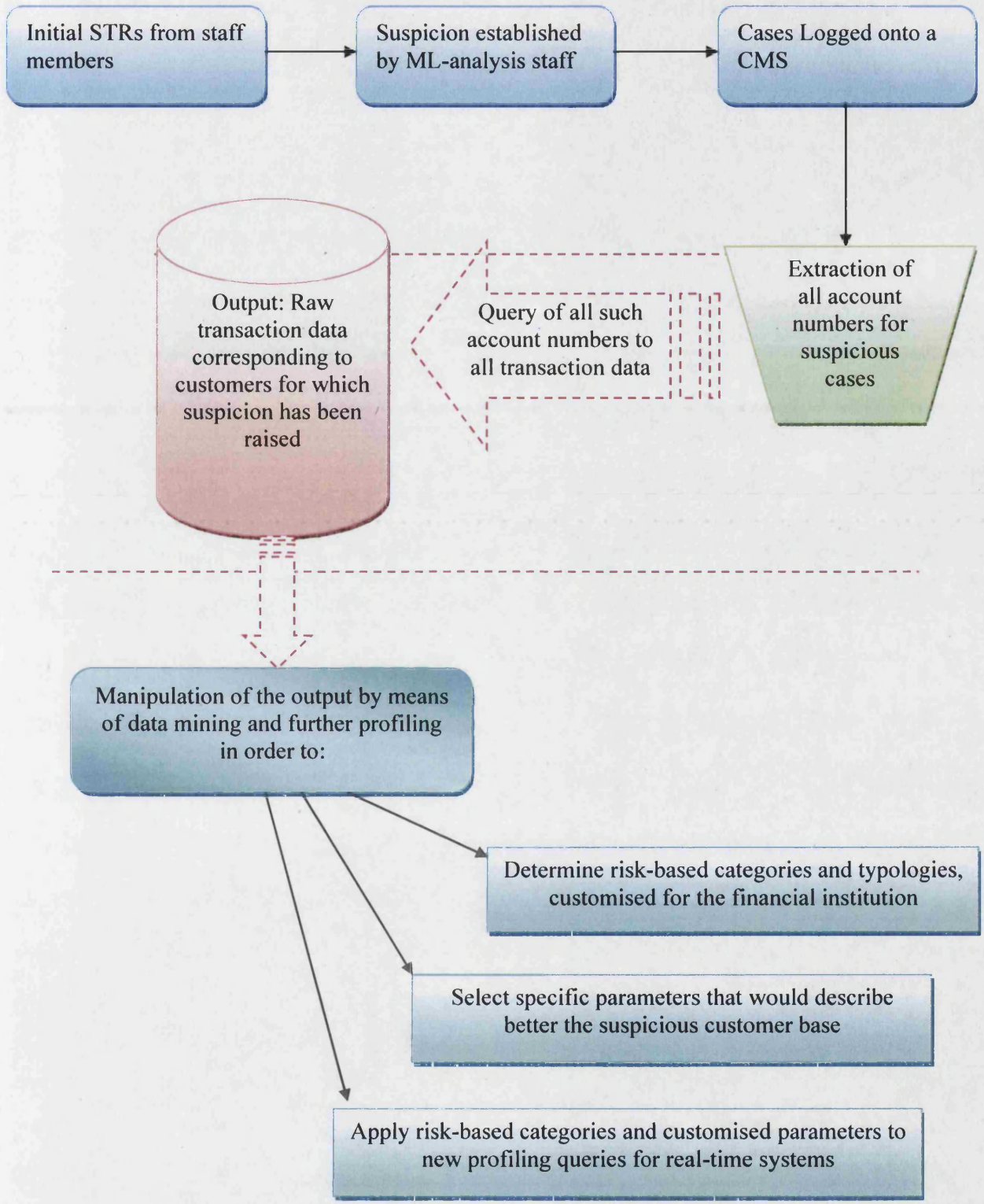


Figure A2. Outline Process for the reverse-engineering of STRs on the basis of raw transaction data from a financial institution

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 that have already been considered suspicious and reported to the FIU are isolated from the greater total transactional sets. In this manner, the reduction in complexity is done 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 250million 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 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 to be relevant to those that have been already reported for suspicion.

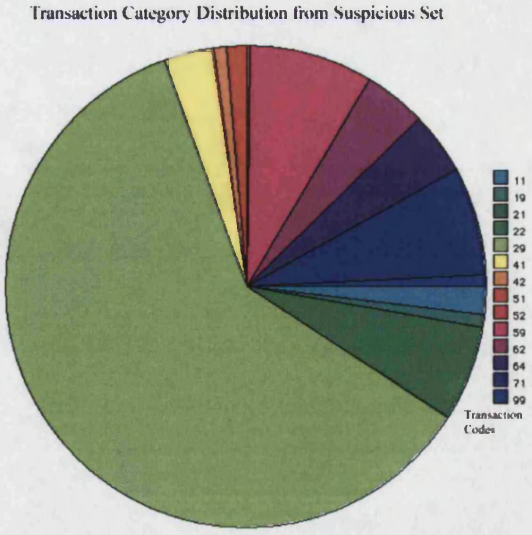


Figure A3. Distribution for transacting categories

Even further, what becomes evident within those transacting categories shown in figure A3 above, is that *from within the subset of transacting categories that appear to be more relevant for money-laundering 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 A3 above, then a probability may be assigned to such a customer; a probability that may quantify the likelihood of someone committing ML. The estimation however of such a probability must not be taken to be linked only with transacting categories. A series of other characteristics can be used for the same purpose (demographic and socio-economic data, etc).

In presenting some of this work in a number of seminars for government agencies in Europe, Central Banks and financial institutions, I have come to realise 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) and it is therefore not something dynamic (whatever 'dynamic' implies).

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 digs considerably deeper into considering 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 customisation 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. Decomposition therefore of those characteristics that are more relevant for the suspicious customers' base of a 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, etc). 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 2nd order observation of the system itself. What makes the difference is that *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. Resolution or even an attempt of manipulating previously known information of other types (such as previous STRs, etc) 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 organizationally and technologically structured. For the example of 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 2nd order observation to take place, another observer must be introduced that will guide another observation. Such a subsequent observation will – via a secondary frame – utilise 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 utilised, 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 the UK 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 utilised 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 beginning of the implementation of automated technologies, the True Positive Rate was less than 1% (*how many reports flagged by technology are considered to be suspicious after further examination).* This has now been improved up to 17% for automated monitoring of suspicion, while for staff members it is much higher at more than 60% (from about 25%).

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. The rate

of increase for a four-year period is shown below in Figure A4, which represents the percentage of Disclosures/Referrals for staff members only. 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/automatic 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, etc). In the figure below the increase in this effectiveness is represented.

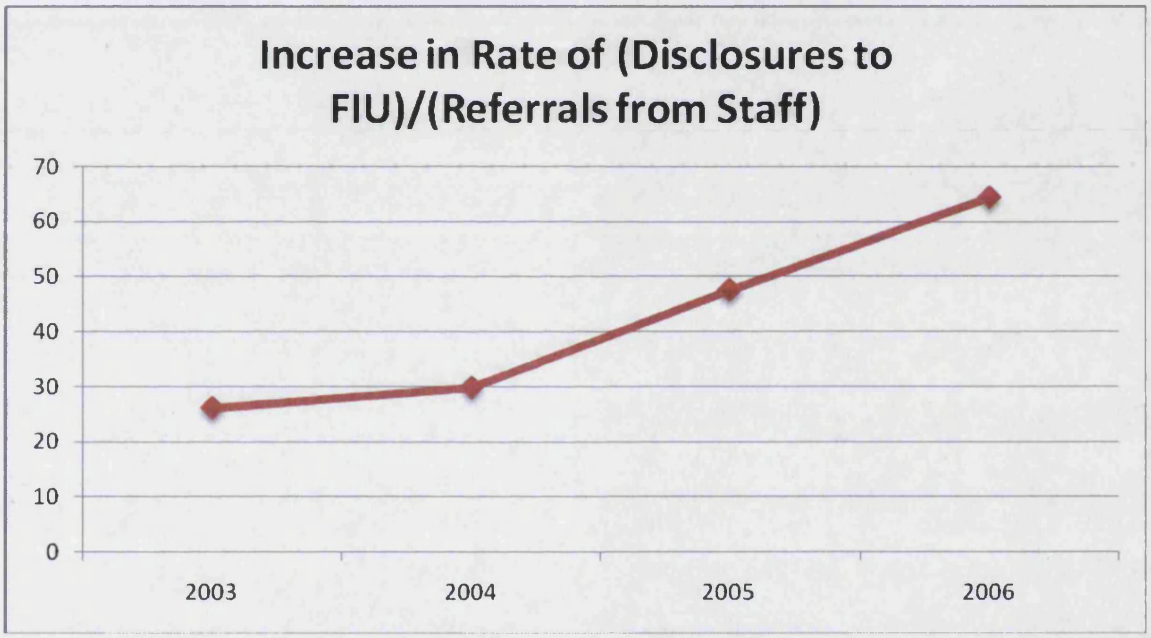


Figure A4. Increase in Rate of Disclosures to FIU/ Referrals from Staff members

With the improvement observed in the example outlined in this Appendix, 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 prioritisation. While I have attempted a deep theoretical treatise on this issue elsewhere[93], I do want to highlight a set of issues that are important.

[93] *The reader may be interested in:* Demetis, D and Angell, I (2007): The risk-based to Anti-Money Laundering: Representation, Paradox and the 3rd Directive. *Journal of Money Laundering Control, Vol.10, Issue 4.*

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 Appendix constitutes both a method for a deeper representation of risk at the level of interaction between different financial transactions, and a recursive mechanism that exploits these financial transactions in tandem with a frame that focuses the observation. This in itself is something considerably different to a simple 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 assume the role of Pythia[94] and hypothesize on the 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

[94] Pythia was the priestess presiding over the Oracle of Apollo at Delphi

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 customise 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 (and I am confident that many of them probably will) while the most important question to ponder will revolve around the self-referential nature of any system and how self-reference can re-inform (and hopefully improve) parts of a system.

As far as technology and AML is concerned I still remain pessimistic (despite the somewhat optimistic tone of this Appendix). The interactions between bureaucracy and electreaucracy, the volume of STRs, and the white noise that comes with them, the difficult problem domain of ML that needs to be simulated, 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% True Positive Rate in automated monitoring implies that from a hundred suspicious transactions that technology generates, only 17 are truly suspicious while an unpleasant 83 remain non-suspicious. Determining whether a flagged transaction (from technology) is suspicious or not requires however manual analysis of the reports, and that in itself implies considerable workload. The problem is unlikely to go away as the nature of modelling ML behaviour is highly complex, and automation is based on the interactive patterns of a myriad information systems that perplex the issue. As e-transacting becomes more and more prevalent, the asymmetry will tend to increase, and it is doubtful whether such a high (!) percentage will be sustainable. It all looks like there is plenty of scope of further research, but then again, that constitutes another self-referential system in itself; research out of research.

References

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. and D. Demetis (2005). "Systems Thinking about Anti-Money-Laundering: Considering the Greek Case." Journal of Money Laundering Control **8**(3).

Angell, I. O. and S. Smithson (1991). Information systems management. London, Macmillan.

Arbib, M. and A. Cornelis (1981). "The role of system theory in the social sciences: an interview." Journal of Social Biological Structures **4**: 375-386.

Aristotle (1957). Metaphysica in Scriptorum classicorum bibliotheca Oxoniensis. Oxonii,, E Typographeo Clarendoniano.

Ashby, W. R. (1958). An introduction to cybernetics. London, Chapman and Hall.

Auerbach, C. F. and L. B. Silverstein (2003). Qualitative data : an introduction to coding and analysis. New York, New York University Press.

Avgerou, C. (2000). "Information Systems: What sort of science is it?" Omega: The International Journal of Management Science **28**: 567-579.

Avgerou, C. and S. Madon (2002). Framing IS Studies, London School of Economics and Political Science - Department of Information Systems Working Paper Series - 112.

Basel. (1988). "Statement on Prevention of Criminal Use of the Banking System for the Purpose of Money-Laundering." from 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 (2003). Consolidated KYC Risk Management, Basel Committee on Banking Supervision.

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

Baskerville, R. (1999). "Investigating Information Systems with Action Research." Communications of the AIS **2**(19).

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**: 417-428.

Berg, B. L. (2001). Qualitative research methods for the social sciences. Boston, Allyn and Bacon.

Bertalanffy, L. (1969). General System Theory. New York, George Braziller, Inc.

Burrell and Morgan (1979). Sociological Paradigms and Organizational Analysis. London, Heinemann.

Checkland, P. (1985). "From Optimizing to learning: A development of Systems Thinking for the 1990s." Journal of the Operational Research Society **36**(9): 757-767.

Christin, I. (1983). "Financial Systems: A few theoretical and algebraic considerations for their modeling." Mathematical Social Sciences **6**: 171-193.

Chua, W. (1986). "Radical Development in Accounting Thought." The Accounting Review **61**: 601-632.

Coffey, A. and P. Atkinson (1996). Making sense of qualitative data : complementary research strategies. Thousand Oaks, Sage Publications.

Cooper, H. M. and L. V. Hedges (1994). The Handbook of research synthesis. New York, Russell Sage Foundation.

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, University of Wales Press.

Demetis, D. (2004). "The World on Discount." The Journal of the London School of Economics SU **3**(1).

Demetis, D. and I. Angell (2006). "AML-related technologies: A Systemic Risk." Journal of Money Laundering Control **9**(2).

Demetis, D. S. and I. O. Angell (2007). "The Risk-Based Approach to AML: Representation, Paradox, and the 3rd Directive." Journal of Money Laundering Control **10**(4).

Dewey, J. (1933). How we think : a restatement of the relation of reflective thinking to the educative process. Boston, Mass. [etc.] ; London, D.C.Heath.

Dimaggio, P. J. and W. W. Powell (1991). The Iron Cage Revisited: Institutional Isomorphism and Collective Rationality in Organization Fields. The New Institutionalism in Organizational Analysis. W. W. Powell and P. J. Dimaggio. USA, University of Chicago Press.

Ditton, J. and R. Brown (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): 521-530.

Duyne, P. v. (1998). "Money-Laundering: Pavlov's Dog and Beyond." The Howard Journal **37**(4): 359-374.

Eisenhardt, K. M. (1989). "Building Theories from Case Study Research." The Academy of Management Review **14**(4): 532-550.

England, C. (2000). Is privetely-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." from 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." from 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. (2003). "What is Money Laundering?" from http://www1.oecd.org/fatf/MLaundering_en.htm.

Feyerabend, P. K. (1975). Against method : outline of an anarchistic theory of knowledge. London, NLB.

Feyerabend, P. K. (1987). Farewell to reason. London, Verso.

Germana, J. (2001). "Emergent Properties: A Fundamental Postulate of Classical Systems Theory in Schematic Representation." Systems Research and Behavioral Science **18**: 565-568.

Geyer, F. (2002). "The march of self-reference." Kybernetes **31**(7): 1021-1042.

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, N.Y., U.S.A., Penguin.

Gödel, K. (1986). Collected works. Oxford [Oxfordshire] , New York, Clarendon Press ; Oxford University Press.

Goldberg, C. and T. Pantos (2003). "The Effects of the EC Banking Directives on Greek Financial Institutions." The Journal of American Academy of Business, Cambridge: 554-559.

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): 102-109.

Greenberg and Goodman (1996). "Is Big Brother Hanging by His Bootstraps?" Communications of the ACM **39**(7).

Hasselbladh, H. and J. Kallinikos (2000). "The Project of Rationalization: A Critique and Reappraisal of Neo-Institutionalism in Organization studies." Organization Studies **21**(4).

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 Advacement of Science. Chaos and Nonlinear Dynamics. Oxford, Oxford University Press.

HKVoD. (1998). "*Hong Kong Voice of Democracy* - Two Chinese Hackers Given Death Sentences." from http://www.democracy.org.hk/pastweek/dec27_jan2/hackers.htm.

Holder, W. (2003). "The International Monetary Fund's Involvement in Combating Money Laundering and the Financing of Terrorism." Journal of Money Laundering Control **6**(4): 383-387.

Hugel, P. and J. Kelly (2002). "Internet Gambling, Credit Cards and Money Laundering." Journal of Money Laundering Control **6**(1): 57-65.

Interpol. (2002). "International Crime Statistics." from http://www.interpol.int/Public/Statistics/ICS/downloadList.asp.

Johnson, J. (2001). "In Pursuit of Dirty Money: Identifying Weaknesses in the Global Financial System." Journal of Money Laundering Control **5**(2): 122-132.

Johnson, J. (2003). "Repairing Legitimacy after Blacklisting by the Financial Action Task Force." Journal of Money Laundering Control **7**(1).

Johnson, J. and D. Lim (2002). "Money Laundering: Has the Financial Action Task Force made a difference?" Journal of Financial Crime **10**(1): 7-22.

Kallinikos, J. (2007). The consequences of information, Edwin Elgar.x

Kaplan, R. and D. Duchon (1988). "Combining Qualitative and Quantitative Methods in Information Systems Research: A Case Study." MIS Quarterly **12**(4): 571-586.

Katsios, S. (1999). "Greek bureaucracy impedes laundering controls." Money Laundering Alert: p.2.

Klein, H. and R. A. Hirschheim (1987). "A comparative framework of data modelling paradigms and approaches." Computer Journal **30**(1): 8-15.

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." from http://www.ncis.co.uk/downloads/kpmgreport.pdf.

Kuhn, T. S. (1970). The structure of scientific revolutions. Chicago, University of Chicago Press.

Lee, A. (1999). "Rigor and Relevance in MIS Research: Beyond the Approach of Positivism Alone." MIS Quarterly **23**(1): 29-33.

Lee, A. (2003). "Systems Thinking, Design Science and Paradigms." from http://saturn.vcu.edu/~aslee/ICIM-keynote-2000/ICIM-keynote-2000.htm.

Lee, A. and D. Demetis (*forthcoming*). "Re-Introducing Systems Theory to Information Systems." MISQ.

Lilley, P. (2000). Dirty Dealing. London, Kogan Page.

Lin, Y. (1988). "Can the world be studied in the viewpoint of systems?" Mathematical Computer Modelling **11**: 738-742.

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. (1998). "Die Gesellschaft der Gesellschaft."

Luhmann, N. (2000). Art as a social system. Stanford, Stanford University Press.

Luhmann, N. (2000). 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. Niklas Luhmann and Organization Studies. S. Clegg and R. Stablein. Copenhagen, Liber & Copenhagen Business School Press: 54-63.

Maguire, S. and B. McKelvey (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. and F. Varela (1998). The tree of knowledge: *The biological roots of human understanding*. Boston & London, Shambhala.

Mayr, E. (2000). What Evolution Is, Phoenix.

McDonell, R. (1998). Money Laundering Methodologies and International and Regional Counter-measures. Gambling, Technology and Society: Regulatory Challenges for the 21st Centure, Sydney.

Miles, M. (1979). "Qualitative data as an attractive nuisance: The problem of analysis." Administrative Science Quarterly **24**: 590-601.

Mitleton-Kelly, E. (2003). Complex Systems and Evolutionary Perspectives on Organisations: The Application of Complexity Theory to Organisations, Pergamon.

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.

Myers, M. D. (1997) Qualitative Research in Information Systems. **Volume**, DOI:

Naylor, R. T. (1994). Hot money and the politics of debt. Montreal, Quebec, BLACK ROSE BOOKS.

Nietzsche, F. (1977). Logic, Epistemology, Metaphysics. A Nietzsche Reader :, Penguin Books.

Orlikowski, W. and J. Baroudi (1991). "Studying information technology in Organizations." Information Systems Research **2**(1).

Philippsohn, S. (2001). "Money Laundering on the Internet." Computers & Security **20**: 485-490.

Pinter, H. (2005). "Art, Truth and Politics." from http://nobelprize.org/literature/laureates/2005/pinter-lecture.html.

Price, A. (2002). Anti-Money Laundering : Reconsidering the Risks. Ernst&Young Monitor Magazine (Strategic Issues for Financial Services Executives). **1**.

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**: 387-398.

Richards, L. (2005). Handling qualitative data : a practical guide. London ; Thousand Oaks, CA, SAGE Publications.

Rider, B. (2003). "Editorial: Who to Trust!" Journal of Money Laundering Control **6**(4): 299-300.

Robinson, J. (1998). The Laundrymen, Simon & Schuster UK.

Ronfeldt, D. (1992). Cyberocracy is coming, Taylor & Francis.

Rossbach, S. (1993). The author's care of himself: On Friedrich Nietzche, Michel Foucault, and Niklas Luhmann. Florence, European University Institute.

Roule, T. and M. Salak (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): 427-452.

Scott, B. (2004). "Second-order cybernetics: an historical introduction." Kybernetes **33**(9): 1365-1378.

Scott, R. (1991). Unpacking Institutional Argument. The New Institutionalism in Organizational Analysis. W. W. Powell and P. J. Dimaggio. Chicago, University of Chicago Press.

Scott, R. and J. Meyer (1991). The Organization of Societal Sectors: Propositions and Early Evidence. The New Institutionalism in Organizational Analysis. W. W. Powell and P. J. Dimaggio. Chicago, University of Chicago Press.

Scott, W. R. (1994). Institutions and Organizations: Toward a Theoretical Synthesis. Institutional Environmental and Organizations: Structural Complexity and Individualism. USA, Sage Publications.

Searle, J. (1995). The Construction of Social Reality, Penguin Books.

Selgin, G. (1994). "On Ensuring the Acceptability of a New Fiat Money." Journal of Money, Credit and Banking **26**(4): 808-826.

Selznick, P. (1996). "Institutionalism "Old" and "New"." Administrative Science Quarterly **41**(2).

Skyttner, L. (1998). "The Future of Systems Thinking." Systemic Practice and Action Research **11**(2).

Spiegel (2007) Sweden Opens Virtual Embassy in Second Life. **Volume**, DOI:

State, D. o. (2001). "An overview of Greece and Money-Laundering." from http://www.state.gov/g/inl/rls/nrcrpt/2002/html/17949.htm.

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**: 338-347.

Trist, E. and F. Emery (2000). Systems Theory and Organizational Change.

UN. (1988). "United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances." from http://www.incb.org/e/conv/1988/index.htm.

UN. (1998). "Attacking the profits of crime: Drugs, Money and Laundering." from http://www.un.org/ga/20special/.

UN. (1998). "Political Declaration and Action Plan against Money Laundering."

UN. (1998). "Political Declaration on Global Drug Control at the UN General Assembly - Twentieth Special Session." from http://www.un.org/ga/20special/poldecla.htm.

UN. (2000). "The United Nations Convention against Transnational Organized Crime." from 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. and Josiah Macy Jr. Foundation. (1950). Transactions of the ... conference. New York, Josiah Macy, Jr. Foundation.

Von Foerster, H. M., G. W. Zopf, et al. (1962). Principles of self-organization; transactions. New York,, Symposium Publications, Pergamon Press.

Walker, J. (1998). "Modelling Global Money Laundering Flows." from http://members.ozemail.com.au/~born1820/mlmethod.htm.

Walsham, G. (1993). Interpreting information systems in organizations. Chichester, West Sussex, England ; New York, Wiley.

Walsham, G. (1995). "The Emergence of Interpretivism in IS Research." Information Systems Research **6:**(4): 376, 380, 384.

West, R. and C. Lebiere (2001). "Simple Games as Dynamic, Coupled Systems: randomness and other emergent properties." Journal of Cognitive Systems Research **1**: 221-239.

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, The World Bank: 45-59.

Xu, L. (2000). "The Contribution of Systems Science to Information Systems Research." Systems Research and Behavioral Science **17**: 105-116.

Yin, R. (1981). "The Case Study Crisis: Some Answers." Administrative Science Quarterly **26**(1): 58-65.

Yin, R. (1984). Case Study Research: Design and Methods. Newbury Park, CA., Sage.

Zemke, R. (2001). "Systems Thinking
Looking at how systems really work can be enlightening - or a wake-up call ." Journal of Training **38**(2).

Zucker, L. (1991). The Role of Institutionalization in Cultural Persistence. The New Institutionalism in Organizational Analysis. Powell and DiMaggio. Chicago, University of Chicago Press.

Endnotes

[i] The evolution of the legislation with the aim of countering money laundering is clearly reflected in the documents that source from various initiatives. The problem of estimating the money laundering market is also a semantic issue because once the definition of what constitutes ML changes according to the legislation, so do the models that pursuit these estimates, in order to incorporate the additionally defined elements according to the norm-producing institutions.

[ii] Interestingly enough, Tanzi (1999) refers to the example of Australia to demonstrate that depending on the methodology that is employed to estimate the underground economy, there can be enormous variations in the estimates like 1.4% to 47.1%. It should be noted at this point that Australia is considered to be the country with the most rigorous legislation and measures against ML and still, it is further estimated that from all the cases that are prosecuted for money-laundering, only 1% of the laundered money can be eventually confiscated [Lilley, P. (2000). Dirty Dealing. London, Kogan Page.] A similar example given by Tanzi is that of the United States where estimates range from 6.2% to 19.4% of the GDP.

[iii] The formulation of an industry that is beyond good and evil partly relies on their interconnectedness and that one cannot exist or be defined without the other (dialectic reasoning). It is also interesting to consider that money-laundering is considered to be a problem *per se*. However, far beyond the arguments that money-laundering is a crime and a problem (mainly sourcing from its connections to drug-trafficking and the fact that it may create another round of crime as it generates money that are subsequently used for illegal purposes), there are some in the literature that do not portray money-laundering as a problem. For instance, it can be argued that money-laundering does not even undermine the status quo. Far from that, 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 the authors argue that people would be more likely to revolt. [Ditton, J. and R. Brown (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): 521-530.
]

[iv] The case of the Chinese hackers was the first case of theft in a bank by remote means but still, a home made modem was installed in the bank's systems. Brothers Hao Jing-long and Hao Jing-wen managed to transfer 720,000 Yuan from the bank. Their attempt to layer their illicit-got profits came by transferring the funds into 16 different accounts they had managed to setup with false names. Having done this, they withdrew 260,000 Yuan from several different branches of the bank.

[v] The typical distinction for the laundering process is done in the placement, layering and integration stages. With CL, the layering stage which is the complication of the money trail in order to blur the origins through complicated transactions, can be done much more easily at the click of a button. Similarly, and if one manages to get a fictitious account in a bank through the latter's online banking systems, the placement stage is also part of the CL. Furthermore, since the placement stage is considered to be the stage where the launderers are more easily caught, the danger exacerbates.

[vi] However, the confiscation of the proceeds of crime remains an extremely touchy subject which once again boils down to the 'who polices the police' quote. Interestingly enough, **the Asian Secretariat of the Financial Action Task Force is self-funded by the confiscated money – Gilmore, W. (1999). Dirty Money: The evolution of money laundering counter-measures. Strasbourg, Council of Europe Press.**

The danger is therefore clear because maximization of government profit might actually lead to confiscating what is convenient. Ethical issues also arise because the same money that sources from criminal activities is used to fund FATF style agencies. Ironically, the agentive function of *legitimate money* is promptly ascribed to criminal money once governments are involved.

[vii] The extent to which money laundering can create economic instability is very difficult to be established. Catherine England suggests that there are several cases where Greesham'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.

[viii] In the 'Customer Due Diligence' work of the Basel committee, risk is categorized in four categories: reputational, operational, legal, and concentration risk. Reputation 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.*

[ix] There are three ways to exchange information: a) **The Mutual Legal Assistance (MLAT)** 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 (however FIU exchange of intelligence is problematic and non-computerized - *dissertation research*), c) **The supervisory channel** where information is mostly communicated for supervisory purposes, specific assets or liability accounts because of risk and reputation concerns (i.e. politically exposed persons).
The three channels are of course complementary and there is a need to co-ordinate between interested governmental bodies within a jurisdiction, and of course across national boundaries.

[x] 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 (and how could they?). 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 black-list?

[xi] The shocking story of the Pentagon selling biological and chemical equipment through the Internet was actually discovered by the 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 government. Interestingly enough, the story was minimally published. Furthermore, it seems that there was a clear policy in the Department of Defence of the United States which prohibited any selling of items. Thus, according to the policy of the DOD it would not have been legal to sell these items. The fact that this occurred shows the degenerate side of capitalism whereby the supposed pillar of the US defence can partially jeopardise national security in order to make profit.

[xii] Attorneys Jonathan Levy and Tom Easton represent Holocaust victims in the Vatican Bank Claims (http://www.vaticanbankclaims.com) as they seek restitution of the illicitly transferred funds.

[xiii] It is interesting to note that concerning the concept of the *paradigm shift* and the notion that Kuhn had developed for that, ST and in particular the version that Professor Luhmann suggests, departs from

Kuhn's description and uses the concept of *systemic differentiation* that is further utilised to describe a paradigm shift. More specifically, and according to Luhmann, whenever a high degree of centralisation of *difference* is being utilised by a great number of observers, then that may constitute a paradigm shift.

[xiv] I wish here to make a differentiation between the importance of an observer and the existence of an observer. Whereas in no one can deny that it takes an observer even to point out any cause-and-effect relations, the identification of *an operation that can be characterised as cause-and-effect* is de-contextualised and hence becomes observer-irrelevant.

[xv] It should not appear confusing at this point that reductionism comes into play. Even within interpretivist research, the fact that many embrace reductionism within the construct of their theories (with Actor-Network Theory being a classic example) while ignoring its consequences at the same time is truly intriguing.

[xvi] 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 the 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 behavior. This again, brings me to a consideration of the AI system at a macro-level, assembled by its sub-systems. There is however a considerable difference that I find here regarding the use of the interactivity between different elements and the projected emergence which I would characterize as elusive. 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.

[xvii] In game theory, it is also 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. and C. Lebiere (2001). "Simple Games as Dynamic, Coupled Systems: randomness and other emergent properties." Journal of Cognitive Systems Research 1: 221-239.

[xviii] 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 subsequently theory construction that have been observed and discussed by Nietzsche (amongst others); that is, a description about one of the most major problems of philosophy whereby something 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 :, Penguin Books.

[xix] Sooner or later of course, 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 conceptualise the thought of the maximum entropy [Heidegger, M. (1994). Basic questions of philosophy : selected "problems" of "logic". Bloomington, Indiana University Press.

[xx] It is indeed important to offer some reflections on complexity and the elements that constitute a system; for 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 here 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.

[xxi] In the scenario examined in the previous footnote whereby information processing can also occur between two abstractions it becomes even more evident that input is internalised. In the scenario for example of the addition between two numbers, then 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 internalised for further information processing).

[xxii] It would be perhaps interesting to say here that when the first Greek Law on Anti-Money Laundering was introduced into the banking sector, the totality of the banking sector appeared to be negative in the reporting of suspicious transactions and for a brief period of time there were no official documentation from financial institutions (the STRs were sent anonymized from the institution and the commitment or signature of an MLRO did not exist as such). Despite the fact that this situation was overturned soon, it accurately portrays the anxiety that senior management displayed over the introduction of the legislation (and its security implications) in the first place.

[xxiii] This brings out the issue of the effects of making fines for non-compliance on AML available to the public. One would expect that the underlying reason for making the fines public has to do with signaling to the market sound competition and letting the market decide how this would affect different stakeholders. In the UK for example and other countries, financial fines for non-compliance on AML are made public but that does not appear to have a considerable effect (unless we are talking about a really serious incident that is re-enforced by other factors as well). What usually happens is that there is a slight drop in the stock market price of the institution, a drop that is however considerably temporal and followed by a quick recovery.

[xxiv] The number of interviews is not mentioned or recorded due to the nature of the research undertaken. I was given an office within the working space of the Money Laundering Analysis Team whereby I had access to the electronic systems provided and used by the team and was given the opportunity to interrupt personnel while they were working to ask about items of investigation, money-laundering issues, etc. In several occasions I was able to interview personnel from the MLAT separately (in another room) if there were items of investigation that required further pondering or analysis. That was required a few items with the Manager and the Deputy Manager of the MLAT of the Bank. Overall, I visited the bank five times (in time intervals that exceeded 3-4 months) with an average of seven days per visit while also being in contact with staff members by telephone interviews for additional items of interrogation. An estimated number of unstructured interviews and discussions concerning AML would definitely be more than one hundred.

[xxv] Even though what information should be collected for the development of 'transaction profiles' was not clearly stated in the KYC policy of the Bank, the intention of such a collection denotes a clear internal will of the Bank to move towards a *profiling* of transactions that will be clearly automated (due to the volume of transactions being carried out).

[xxvi] From the point of view of the Financial Intelligence Unit this becomes even more problematic as different financial institutions also require different Identification documents sometimes. This was a problem that several financial institutions were facing as well because 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.

[xxvii] Live systems of course create other problems but this particular aspect here opens another important element in the discussion concerning Anti-Money Laundering. The fact that there is no time-limit restriction that would justify a suspicious transaction report towards the Financial Intelligence Unit means that the possibility remains open that various financial institutions would willingly accept the proceeds of crime and then also report an STR. If the legal obligation is only towards reporting suspicion then this becomes inevitable that to some degree financial institutions have the flexibility of passing on the problem (and the volume of suspicious transactions) to Financial Intelligence Units while at the same time dealing and/or investing the proceeds of crime that they have received. This issue of *timeliness* in reporting a suspicious transaction remains of course elusive but it is an issue that has been given some additional attention recently through the 3rd Anti-Money Laundering Directive.

[xxviii] The online system requires authentication from both the teller and the chief teller so that the teller can carry out transactions. Everything is recorded and kept for a considerable amount of time.

[xxix] 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 and Police ID number or Tax Number, then that would be flagged out as a positive match and the case would be further investigated so that multiple accounts could be united into one number in the POSEIDON system.

[xxx] I am not making a value judgment here at all. As it will become obvious, my position on automated systems for Anti-Money Laundering is not one of superiority pertaining to their imposition from regulators.

[xxxi] XML – Extensibility Markup Language – is useful in facilitating the sharing of information across different infrastructures as it allows for users to share data between them, and also to define their own elements.

[xxxii] The fact the one alludes to a description like 'combating the phenomenon of money-laundering' points at exactly the problem of philosophical atomism and the difficulty in recognizing the unavoidable differentiation that occurs within the domain once *observation* commences to examine aspects of the problem domain itself. This means that the phenomenon of money-laundering is treated as a unity whereas it can only be treated as such at the level of other subsystems at the same level with which ML is structurally coupled (like AML).

[xxxiii] It is interesting to note that studies have emerged in the field of crossing *power* and the constitution of AML within a Foucaultdian perspective