RESEARCH PAPERS OF WROCŁAW UNIVERSITY OF ECONOMICS No. 104
Business Informatics 16 2010

Dionysios S. Demetis
London School of Economics, London, United Kingdom
d.demetis@lse.ac.uk

ARTIFICIAL NON-INTELLIGENCE AND ANTI-MONEY LAUNDERING

Abstract: This paper deals with the popular belief that a technological solution for the domain of money laundering is possible; the paper takes an opposing view by examining some of the complexities underpinning the modelling of the problem domain and postulates some general systemic properties that are acting against any concept of "solution". While a number of computational techniques have been advanced for the profiling of money laundering behaviour, the algorithmic representations behind the queries cannot effectively reduce the complexity of the phenomenon. While these approaches are useful for financial institutions that wish to demonstrate compliance, they fall short of expectations. Complex human behaviour cannot be easily modelled and the intrinsic risk in any act of computational categorization is passed on as yet another layer of complexity.

Keywords: money laundering, profiling, technology, risk, systems theory.

1. Introduction

From the very outset of this paper, let me first explain the somewhat bizarre title. I do not mean to be offensive to the computer science community by proclaiming that technology is of no use, simply because artificial intelligence has not lived up to the hype of the last decades. I merely imply to set out a link between the reckless utilization of technology (in all of its forms) within the domain of anti-money laundering. I also mean to establish the systemic nature of a non-solution to the problem domain of AML. Whereas all sorts of algorithms have been employed for the profiling of money laundering behaviour, they have all radically failed as the logical presuppositions upon which computations are performed are everything but intelligent. Intelligence in this regard is not a logical property of any system [Angell 1993]; it is a biological characteristic that we attempt to simulate, albeit unsuccessfully [ibid.]. This is because of fundamental epistemic, ontological, as well as philosophical problems. Every categorization is an act of choice, an imposition of a distinction that is guided by an observer; as such, any simulation is based on the presuppositions of the distinctions it engulfs. It remains an act of choice and devoid of the intrinsic complexity that is present of any system.

2. The general issues

Three major themes have always stood important whenever there were any discussions regarding the integration of technology to the fight against ML. The first theme has to do with the huge mass of data that financial institutions have to cope with. For instance, a large financial institution in the UK deals with about 15-20 million transactions per day [Gate 2008]. Months of raw financial transaction data create a huge database. Checking those transactions for money laundering behaviour becomes really difficult. In any event, this mass of data has created the need to carry out computerised profiling and deal with the data in an automated fashion. Technology *becomes* of use because the volume of transacting forbids manual manipulation of the data.

Such a vast mass of data feeds forward to the second theme that attempts to exploit any relationships between data [Demetis 2009]. The problem here arises in the construction of the profiling queries themselves; queries that are developed to model ML [Backhouse et al. 2005]. Are the relationships uncovered by profiling meaningful? Or is it simply that the relationships are imposed by the profiling queries in the first place? If one tries hard enough, she or he will always find "meaningful" relationships in the data. To the extent that these actually help in decision-making, increasing effectiveness and efficiency, and ultimately demonstrating compliance, remains an issue subject to considerable debate.

But if one were to ask how much profiling and data-mining has helped the world of anti-money laundering, the answer would probably be to the negative. The concept of the "pixie-dust school of technology" is heavily related to this matter. Business managers, compliance officers, politicians, all usually operate under the belief that you can sprinkle technology on a problem domain (like a pixie-dust) and make the problem go away magically. There are numerous examples in the fields of identity [Fidis 2005, 2009; Nabeth 2005], terrorism [Tupman 2009], security [Backhouse 2002; Dhillon, Backhouse 2000], etc. In fact, all modern institutions have been completely transformed with the assistance of technology. But technology is now also part of the blame-culture. A form of an intermediary that is to blame.

Financial regulators around the world wanted "systems in place". Financial institutions globally were forced into a swift adoption of anti-money laundering software. The software industry around AML, Profiling, Fraud, AML training, Compliance, and so on, came out booming. A few years ago there were only a few companies providing IT solutions for these areas but now there are too many to mention. As Chekhov said, "when a lot of different remedies are suggested for a disease that means the disease can't be cured" [Chekhov 1991]. And indeed, a number of remedies have been suggested. AML software like Norkom, Unisys, Mantas, Searchspace, etc., to name but a few. But the problems ever since the introduction of AML software persist.

A brief example comes from data discussed with the head of an AML group from one of the biggest financial institutions in the Balkan area. Their financial institution bought and installed an off-the-shelf software platform. Following the installation of the software and after months of efforts, the software is currently producing about 2,000 Suspicious Transaction Reports per day! Actually, it produces more than that but the graphical user interface of the software allows the viewing of the first two thousand and no one has bothered looking beyond that. But while the STRs are coming in the thousands, manual analysis of the reports by ML-analysts is limited to roughly 100 STRs per day. The rest are thrown away rather casually. They are considered to be background, or white noise, an annoyance to the method of producing real suspicious reports. The question here is simple: How do you select the 100 from the 2,000? The answer is that you are supposed to perform some sort of risk-scoring of the customers, and select those with the highest risk. In other words, you are supposed to apply some form of a risk-based approach, another constructed delusion in the world of anti-money laundering stemming from the fundamental misconception that risk can actually be modelled and quantified effectively [Demetis, Angell 2006, 2007].

After the software has supposedly done its job in producing suspicious reports and after ML-analysts clear out the mess and decide which of those are actually suspicious, we are left with what is known as the True Positive Rate. This Rate indicates what percentage of the software-generated suspicious reports are considered to be really suspicious after manual examination of the reports takes place by analysts. In this particular financial institution this number was approximately 0.02% running on one of the latest – and highly expensive – AML software claiming to be using a mix of the best algorithms available for spotting the suspicious transactions. Of course, while this percentage of the true positive rate is extremely disappointing, it is far from unusual. In fact, most financial institutions start off with TPRs at this range and gradually manage to increase them (at roughly 5%) after years of manipulation and fiddling with the queries that support the spotting of suspicious transactions. Even the financial regulator in the United Kingdom suggested that the industry average of the TPR rate should be about 4-7%. In other words, for every 100 suspicious reports that the technology generated, 4-7 reports alone would be considered as really suspicious after careful manual examination by ML analysts. Despite all the expertise available and all the evolutions in constructing supposedly sophisticated algorithms for the spotting of suspicious transactions, even official suggestions fall short; but they do reflect the reality behind the problems of using software for money laundering detection. Of course, ask any computer scientist and he/she will have a solution; a more advanced algorithm, a more advanced computational technique, a new modelling approach, etc. The reality is that financial institutions are tired of experimenting with all these sophisticated techniques that do not work and cost a lot of money. The culture is changing rapidly to one of plain compliance (what is strictly required and not what could really be done to improve the conditions for tackling the phenomenon). Evidently, the introduction of the risk-based approach has an important role to play in this as what is compliance to ML-regulations is now prone to considerable malleability.

3. The complexity of the domain

The question is why is it so difficult to model money laundering? Why is it so difficult for technology to assist in the fight against ML? Why is technology causing so many problems across a wide number of stakeholders in AML (and not just financial institutions)?

First of all, money laundering is an evolving structure and the typologies are interconnected with the facilities that are provided for the movement of money. These are changing rapidly. The nature of money is changing rapidly as well. One such example is *virtual-cash*, surfacing in the last few years in what is known as MMORPGs (standing for Massive Multiplayer Online Role Playing Games) [Damer 1997; Schroeder 2001; Taylor 2002]. Of course, way before virtual-cash was introduced, private money has always been preferred to government money but as soon as it emerges, governments act quickly to suppress it for control purposes. The example in China with the infamous QQ coins speaks for itself. This virtual currency became so popular that real retail shops started accepting it. Only swift action by 14 ministries including the Central Bank of China prevented widespread use of this currency that was feared to destabilize the legal currency of the country and harbour money laundering [Fowler, Qin 2007].

Secondly, ML is the world's third largest market, after the domestic US bond market and the Eurobond market. This creates a volume and an interconnectedness that follows market rules. Money laundering becomes a commodity and therefore those that provide it must compete on price. Underground competition increases variation in the scope of the availability of laundering networks. The networks of Hawala are a typical example where all that is required is a fundamental basis of trust.

Thirdly, the facilitation of electronic transactions and electronic banking in general, have radically changed the fight against ML. If one considers that only 25% of the world's population is currently online and that the percentage of population with access to e-banking facilities is even less, then it is evident that there will be profound long-term consequences which have yet to be soon.

Finally, the economic aspect of globalisation has forced countries into a trade openness that, according to the International Monetary Fund is unavoidable. Trade openness is now inextricably linked to economic growth and hence the economic aspect of globalization, broadens the interactions of financial participants, creates more complex networks of transacting, and within those complex networks lay the possibility of scaling ML to a higher level. Tracking the money-trail for ML investigations becomes even more difficult.

4. The efforts of financial institutions

Financial institutions have indeed been trying (or have been forced into trying). They have invested heavily in compliance and hence compliance costs have been increasing rapidly. In the US alone, it is estimated that about $20 billion have been spent in the past 5-6 years, to comply with anti-money laundering regulations. At one stage, this need to comply generated considerable unease at financial institutions. As a Money-Laundering Reporting Officer (MLRO) from a US bank mentioned to the author of this paper, money were taken out of investments, and were put aside to pay for potential future fines from FinCEN, the US regulator. This is not peculiar. Any government – the unproductive institutional basis of an economy – will try to find more and more ways to get money from the institutions and individuals that are under its control. Taxation is one matter but decades of reinforcement mean that it has become institutionalized. The new trend is imposing regulations and then fining stakeholders for non-compliance. In a sense, regulation has become a *Denial of Service Attack* on business. Here is at least one common point between government practices and computer security literature.

The institutional setting did not use to be like that. The rules are now constantly changing: technology makes it convenient and easy. With information systems, data is stored on the databases of financial institutions and other stakeholders, and sooner or later regulators and mostly FIUs will demand some sort of access. This is a classic example in Italy where the Italian FIU receives all the raw financial transaction data from all financial institution in Italy – in aggregate form, every 3 months. These are stored in a single database also known as the "Archivio Unico Informatico" and are manipulated in order to uncover money laundering incidents.

The extent of such regulatory-initiatives is evident in various national contexts but hasn't had the desired effects that everyone was hoping for. A low rate of both prosecutions and assets recovered is observed, whereas the costs incurred to carry out recovery remain high. In France for instance, it has been reported that only 4% of the submitted suspicious transaction reports were pursued by prosecutors, while in Australia, a country that is supposed to be employing highly rigorous measures, only 1% of the laundered money has eventually been confiscated.

At the same time, and in different national contexts, stakeholders are often operating in isolation, with little consideration of the broader issues. It goes without saying that every institution has got its own agendas to follow, and these in their turn are influenced by their respective institutional backgrounds. There is a need to overcome such fragmentation and while several attempts have been made towards that direction from supra-national organizations, the problems still linger.

5. The disorder of technology

As it has already been alluded to in the very beginning of this paper, the problems that have been created by the introduction of technology to different aspects and different levels of the broader Anti-Money Laundering system have created considerable problems. Contrariwise to those that advocate the orderly fashion with which technology influences a problem domain, the reality is much different. The disorder of technology has found its way in many occasions and the reason is fairly simple.

Those that either impose the functionality of technology or those that incorporate technology within business processes do not often realise that when technology interferes with human activity systems, potential disasters are unavoidable. What they do not understand is the critical difference between cost and price. With every introduction of a technology there is a price to pay, but there is also a cost to suffer. Whereas price is here and now and can usually be easily estimated, the cost often accrues from here to eternity. NASA Astronaut Mike Collins certainly got the difference between price and cost straight, when he referred to the risk of a space mission and the risk of something going wrong. When a journalist asked him what was on his mind during the blast-off of the space-shuttle, he replied that "you are on top of 6 million parts, all made by the lowest bidder".

Collins' comment also points to the uncertainty of combining different technologies together. Indeed, within a few years time of introducing technology to AML, technology has been largely responsible for a series of things. More specifically, technology has been responsible for creating vast amounts of suspicious transaction reports that were generated with the help of 'intelligent' software. As the Know Your Customer principle, the testing capacity of a financial institution is limited, it becomes obvious that it is impossible to scrutinize all the suspicious transaction reports that the software generates. Three underlying processes were uncovered behind that particular problem.

1) Either the financial institutions would report nearly all the transactions that the software deemed suspicious,

2) or they would hire more staff to handle the volume of the reports,

3) or far more interestingly, they would adjust the profiling queries in such a way so that the volume of the results could match the capacity that the institution had for further manual analysis and examination. Undoubtedly, this was very witty from an organizational perspective of dealing with the problem domain, and at the same time, it illustrated in ample terms the deficiencies of introducing AML-related technologies in the financial institutions.

A severe and direct consequence was experienced as a result of the above practices, mostly referring here to the issue of over-reporting. The databases of Financial Intelligence Units (i.e. the organizations responsible for collecting the suspicious transaction reports for money laundering) were filled with white-noise. Instead of useful information that could initiate an investigation and even a prosecution of money laundering, the FIUs ended up receiving useless information. In all of these processes, technology has played an important role because it gave the tool to the financial institutions to report excessively. It was specifically this problem that led – much later – to the introduction of the risk-based approach by the 3rd Directive of the European Union. That introduction alone is meant to reduce the compliance-fear experienced by the majority of financial institutions (accompanied with a series of financial fines for non-compliance) and indirectly to maximize the potential for useful submissions of STRs. Nevertheless, despite the intentions, this approach has led to considerable confusion because of the ambiguities intrinsic in the concept of risk itself.

The story with Anti-Money Laundering software is archetypal of the problems that the introduction of technology has caused for other stakeholders within the AML domain. This is clearly reflected in the effectiveness of the broader AML system. For example, in the UK it was estimated a few years ago that £250 billion were laundered in the UK alone. This is of course a rough estimation, as are all estimations on the extent of money-laundering [Tanzi 1999]. What we do know however is that from these £250 billion, the amount of money that was confiscated was £46 million. The problem is that the cost of investigation for confiscating this £46 million, was £400 million!

As for any "intelligent" profiling software, it quickly became evident that it was usually overloaded with functionality that nobody needed. Software companies had to justify the excessive costs and in some cases bundled up to 100 predefined queries for spotting money laundering behaviour. In reality only few were used, about 5 or 6. This is still the case in the majority of the financial institutions. And without going into details about the content of the queries themselves or their formulation, it would suffice to say that they were fairly simple and straightforward, most of them focusing around a number of parameters like the time of association of a customer to the financial institution, age, location, etc., along with some standard typologies for ML provided by the Financial Action Task Force. In fact, for most practical purposes financial institutions required when dealing with AML, the job could have been done with open-source (i.e. free) software. For instance, the MySQL open-source database platform along with its query construction tool could have been used. The particular platform numbers more than 6 million installations including NASA, Yahoo, the Associated press and many others. Only NASA is saving $4 million annually from switching to this open-source platform after dropping Oracle. Where such an approach fails however is in its legitimacy. By spending a vast amount of money, albeit unnecessarily, does demonstrate to the world of regulators a strong will to compliance who see correlation between spending and efficiency.

But no matter what one does, there is only one inescapable conclusion and only one transcendental property in all systems including AML: *complexity*. Complexity always finds its way around any system; it may change form and shape or even philosophical underpinnings, but hardly looses its characteristics as complexity. In this manner, logical complexity transforms into mathematical complexity, then onto algorithmic complexity, then onto profiling complexity, and even into visual complexity while one tries to carry out data-mining by visual examination of datasets. From a systems theoretical approach this is all perfectly understandable because no system can escape the intrinsic complexity of the elements that constitute it [Luhmann 1990, 1995, 2002].

An alternative approach is by conceptualizing a behavioural modelling approach where the contextualization of different behaviours ranges from banking to business, then on to criminal, and lifestyle. The parameterisation of individual elements within each of these behaviours with selected combinations between them becomes highly interesting. How such behaviours "balance", what roadmap should help in guiding the financial institutions for doing this, and how the combinations between them should be considered, are all issues of immediate concern [Spotlight 2006; Gate 2008].

6. The function of technology

The remarks discussed above point towards an important distinction that remains at the centrepiece of all problematization on AML/ML. Technology is often viewed outside of its organizational implications and the consequences that are created when *an automated function (like that of technology)* re-arranges the already-present bureaucracy of an organization. But this is only part of the problem. Technology is also viewed as a solution that – when imposed onto the problem domain of money laundering – will somehow ameliorate the difficulties of spotting the suspicious transactions. Such a belief is flawed because it bypasses the *contextual* use of technology. Had technology been operating in isolation, then the "blue-sky thinking" of constructing a "more intelligent" artificial mechanism for dealing with the problem would not have mattered. But the integration of technology within an organizational setting has implications that stretch beyond the best of intentions/expectations of computer programmers.

The deep penetration of technology within most contemporary modern institutions has granted computer science with the delusion of causality. Whereas technology (e.g. software) is designed in order to address particular business problems, the analysis of these problems to begin with, is based upon a *necessarily* distorted concept of the "problem". It is actually believed that there is *a problem* and that there is *a solution*. This structural coupling between *problem*/*solution* constitutes a paradox that has been the subject matter of discussion by many academic authors.

In fact, viewed systemically this would be a contradiction within systems theory, which dismisses cause-and-effect relations. This must be made clear. 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.

There are no solutions; only contingencies. When it comes to any type of technology being embedded within an organizational setting, these contingencies give rise to an emergent information system that resists formal attempts at its manipulation. It interacts with the pre-established basis of other information systems, and at the same time, it constructs part of the organizational "reality" thus giving rise to unintended phenomena for other stakeholders operating in the environment of an institution. One such instance was the example given of the impact of technological integration in financial institutions and how it has affected the receiving end of Financial Intelligence Units.

While technology has undoubtedly assisted in the manipulation of large datasets, a manipulation that would not have stood possible by manual means, it has also created severe interferences in the organizational structures that have incorporated it. Even though the belief that there can be an improvement in the algorithms that detect suspicious transactions will not easily be diminished, it remains essential that those that are engaged in the profiling of suspicion for ML, equip themselves with a better understanding of the organizational and contextual issues surrounding the introduction of AML-software.

References

Angell I. (1993), Intelligence: logical or biological, *Communications of the ACM*, Vol. 36, No. 7, pp.15-16.

Backhouse J. (2002), Assessing certification authorities: Guarding the guardians of secure e-commerce?, *Journal of Financial Crime*, Vol. 9, pp. 217-226.

Backhouse J., Demetis D.S., Dyer B., Canhoto A., Nardo M. (2005), *Spotlight: New Approaches to Fighting Money-laundering*, http://www.spotlight.uk.com.

Chekhov A. (1991), *The Cherry Orchard*, Dover Publications.

Damer B. (1997), *Avatars! Exploring and Building Virtual Worlds on the Internet*, Peachpit Press, Berkeley, pp. 7-9.

Demetis D., Angell I. (2006), AML-related technologies: A systemic risk, *Journal of Money Laundering Control*, Vol. 9, No. 2, pp. 157-172.

Demetis D.S. (2009), Data growth, the new order of information manipulation and consequences for the AML/ATF domains, *Journal of Money Laundering Control*, Vol. 12, No. 4, pp. 353-370.

Demetis D.S., Angell I.O. (2007), The risk-based approach to AML: Representation, paradox, and the 3rd directive, *Journal of Money Laundering Control*, Vol. 10, No. 4, pp. 412-428.

Dhillon G., Backhouse J. (2000), Information system security management in the new millennium, *Communications of the ACM*, Vol. 43.

Fidis (2005) D3.2, *A Study on PKI and Biometrics*, Eds. M. Gasson, M. Meints, K. Warwick, http://www.fidis.net

Fidis (2009) D17.1, *Modelling New Forms of Identities: Applicability of the Model Based on Virtual Persons*, http://www.fidis.net.

Fowler G., Qin J. (2007), QQ: China's New Coin of the Realm?, *The Wall Street Journal*, http://online.wsj.com/public/article/SB117519670114653518-FR_svDHxRtxkvNmGwwpouq_hl2g_20080329.html.

Gate (2008), *The GATE-Project on Anti-Money Laundering and Terrorist Financing* (funded by the European Commission on Security Research).

Luhmann N. (1990), *Essays on Self Reference*, Columbia University Press, New York.

Luhmann N. (1995), *Social Systems*, Stanford University Press, Stanford.

Luhmann N. (2000), *The Reality of the Mass Media*, Polity Press, Cambridge.

Luhmann N. (2002), *Theories of Distinction: Redescribing the Descriptions of Modernity*, Stanford University Press, Stanford.

Nabeth T. (2005), Understanding the identity concept in the context of digital social environments, *CALT-FIDIS Working Paper, January 2005*, http://www.fidis.net.

Rossbach S. (1993), *The Author's Care of Himself: On Friedrich Nietzsche, Michel Foucault, and Niklas Luhmann*, European University Institute, Florence.

Schroeder R. (2001), *The Social Life of Avatars: Presence and Interaction in Shared Virtual Environments*, Springer, London, pp. 3-31.

Spotlight (2006), *New Approaches to Fighting Money-Laundering*, London School of Economics, London, http://www.spotlight.uk.com.

Tanzi V. (1999), Uses and abuses of estimates of the underground economy, *The Economic Journal*, Vol. 109, pp. 338-347.

Taylor T.L. (2002), Living digitally: Embodiment in virtual worlds, [in:] *The Social Life of Avatars: Human Interaction in Virtual Worlds*, Ed. R. Schroeder, *Springer*, *London* pp. 40-62.

Tupman W.A. (2009), Ten myths about terrorist financing, *Journal of Money Laundering Control*, Vol. 12, No. 2, pp. 189-205.

NIESZTUCZNA INTELIGENCJA I PRZECIWDZIAŁANIE PRANIU PIENIĘDZY

Streszczenie: autor, argumentując złożonością modelowania procesu prania brudnych pieniędzy, przeciwstawia się powszechnej opinii, że rozwiązanie tego problemu leży w sferze technologii informacyjnej. Proponuje ogólne systemowe własności, które są w stanie konkurować z tzw. rozwiązaniem technologicznym. Podczas gdy techniki informatyczne pozwoliły na określenie profilu zachowań piorących brudne pieniądze, to reprezentacja algorytmiczna kwerend wcale nie zmniejszyła złożoności tego zjawiska. Podejścia te, użyteczne dla instytucji finansowych, które pragną ukazać ich przydatność, nie spełniają pokładanych w nich oczekiwań. Złożoność modelowania zachowań uczestników tego procesu oraz ryzyko błędu procedur obliczeniowych powodują, że zadanie wykrycia operacji prania brudnych pieniędzy staje się jeszcze bardziej skomplikowane. W pracy przedstawiono wiele przykładów potwierdzających tezę autora artykułu.