

“Information processing and decision making in financial intelligence – a semiotic approach to financial crime investigation”

Authors:

Ana Isabel Canhoto, London School of Economics, a.i.canhoto@lse.ac.uk

Dr. James Backhouse, London School of Economics, james.backhouse@lse.ac.uk

Abstract. Much crime investigation today is carried out by automatic scrutiny of large transaction databases, with considerable value placed on the use of profiles to seek out unusual and potentially suspicious behaviour. However, the power of automated profiling can result in negative outcomes such as over-reporting and increased expenditure on manual compliance checking. This paper examines some of these problems using a semiotic framework that draws attention to the delicate interplay of technical and social factors in the search for both efficiency and effectiveness. The framework involves a six level semiotic model through which each level permits a focus on different elements of concern for how agents identify signs and create meaning within a normative context. Instead of the prevailing assumption about a simple flow of information from financial institution to Financial Intelligence Unit and prosecuting agency, this approach suggests that the identification and communication of suspicion is a more complex and social process whose nature should be better understood.

Introduction

The report of the United Nation’s High-Level Panel on Threats, Challenges and Change, published in early December 2004¹ underlines the point that in today’s interconnected world a threat to one state’s security is a ‘threat to all’. The report also mentions that terrorism has important economic consequences worldwide, as illustrated by the attacks of September 11th 2001, in the United States which, according to World Bank estimates, cost more than \$80 billion dollars and pushed 11m people in developing countries into poverty (Annan, 2004).

The collection and analysis of financial data, referred to as financial intelligence, is gaining recognition as a key tool in the war on crime in general and terrorism in particular. Money in electronic form leaves a trail which means that individuals cannot easily disappear (Levi and Wall, 2004). There is a burgeoning industry providing sophisticated computer technology and complex mathematical models to mine financial data and single out unusual patterns of transactions. The use of automated monitoring systems is often seen as a powerful ally in the fight against money laundering and terrorist financing, justified by the increase in size of the typical transactional database, and by a desire to keep compliance costs under control.

It is important to keep in mind, however, that electronic databases and software can only facilitate the work of the investigators, not replace it (Gleason and Gottselig, 2004). The technical systems save countless hours in assembling and processing data. However, automated alerts are of merely ‘unusual’ activity, which still requires further analysis to determine whether there is anything suspicious. It is only after the analysis by financial investigators that such patterns are eventually deemed suspicious or reflecting criminal behaviour. The construction of the identity of a money launderer or a terrorist financier requires from the financial investigators a complex balance between computerized risk assessment models and personal judgment of the motivations behind specific observed financial behaviour. The consequences of a mistake are profound: waste of valuable resources if the case is a false positive, inability to capture a criminal – and, eventually the loss of lives - if the case is a false negative.

We compare the intelligence building process to an act of communication between three levels that are very different in nature: 1) the technical level that captures and manipulates the data, 2) the informal level of human interactions in the process of giving meaning to the data provided by the technical level and acting upon this knowledge and 3) the formal level of the organisation where these agents participate.

¹¹ Available at www.un.org/secureworld

We argue that the process of creating and disseminating intelligence is not the discovery of an 'objective' truth, in which the 'methods' are neutral techniques (Bisman and Hardcastle, 1999, Punch, 1998) separated from the personal positioning of the investigator. Rather, we argue, 'subjectivity matters' (Riessman, 1994). The personal and organizational circumstances surrounding the agent, including perceptions and organizational values may influence how specific intelligence is perceived and communicated. When organizations make decisions, they must take into account that different perceptions are brought in by different interested persons (Liebenau and Harindranath, 2002).

The paper addresses the social aspects of the creation and use of information, in the context of the fight against money laundering and terrorist financing. We suggest that, instead of merely adding to the battery of technology and regulation that already exists in this field, financial crime investigation efforts might find profit in considering social and pragmatic aspects of intelligence building. The present approach is informed by organizational semiotics, a theoretical framework that addresses the creation of meaning in an organizational setting (Liebenau and Backhouse, 1990, Stamper, 1973).

A case study of collection, analysis and dissemination of information regarding a suspected case of money laundering underpins an analysis of how social factors interact with technology, in the decision making process regarding the classification of specific patterns of financial behaviour as suspicious of money laundering.

Theoretical Framework

Charles Peirce developed the field of semiotics² as a 'formal doctrine of signs' (Peirce, 1931-58). It addresses the creation, processing, use and effects of signs. It enables us to understand how meanings are made (Sturrock, 1986), and how information flows from data to an actionable event.

Several semiotic models were developed from Peirce's work for specific applications. Of particular relevance to this study is Organizational Semiotics (Liu, 2000), a body of theory that addresses how the surrounding culture in which the agents participate influences the way in which they create meaning. It incorporates the social and organizational aspects of information, as well as the technical ones.

The research community around this model adopts the subjectivist paradigm as its philosophical stance. This assumes that reality is created subjectively and socially, leading to subtle differences between groups of knowing agents. Additionally, it considers that 'meaning' is the relationship between a sign and some pattern of action, and that this relationship is established as a norm within a given group (Stamper, 1993).

The implication for the researcher in the fields of communication and information systems is that language and linguistic labels are not only descriptive tools, but also constructive ones: the use of language can have the effect of constructing or altering the social world (Searle, 1969, Searle *et al.*, 1980), and can create new states of affairs perhaps just through the deployment of a sign (Austin, 1980). To study the social world, the researcher must first understand the way in which the members of a society create, modify and interpret the world to which they belong. The agent is responsible for the existence of a sign and its meaning (Liebenau and Harindranath, 2002).

Organizational semiotics analyses information along six levels:

Level	Focus
Physical	Physical aspects of signs
Empiric	Properties of signs when different media and devices are used
Syntactic	Formal or structural relations between signs
Semantic	Relationship of signs to the actions to which they refer
Pragmatic	Relation of signs to interpreters
Social	Effects of the use of signs in human affairs

Table 1. The semiotic ladder

The *physical*, *empiric* and *syntactic* levels are suitable for understanding the issues concerning the technical platform for the communication act. The analysis of information at these three levels will be

²² The word "semiotics" has its origin in the Greek work for "symptom" which means something that indicates the existence of something else, for example, a disease.

primarily focused on the effect of the uncertainty caused by the noise and distortion inherent to the channel being used, in the certainty of the message. It is critical for assessing whether the message has reached its destination.

The *semantic*, *pragmatic* and *social* levels look at issues concerning the communication between individuals - that is, the social side of communication. It takes into account issues such as culture, intentions and signification, and analyses how such issues might impact on the ability of the receiver of the information to, not only understand the message, but also the sender's intentions.

The relevance of the theoretical framework to the study of the creation and use of information is summarized in figure 1.

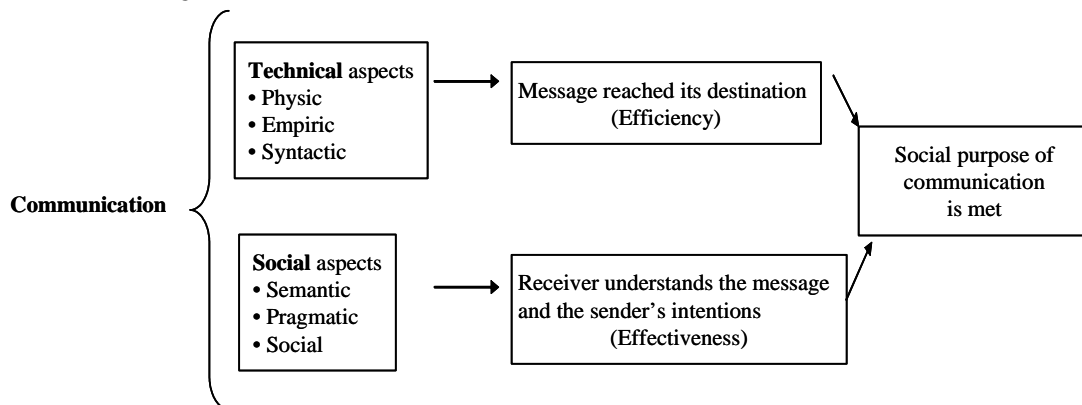


Fig. 1. Research Framework

Technical aspects of communication

Information theory holds that communication is reliant on a channel that transmits signals between an information source (the sender) and an information destination (the receiver) (Shannon and Weaver, 1949). The channel is subject to noise and distortion which corrupts the integrity of the message. This section looks at the characteristics of the signal and the channel, reflecting on possible sources of disruption.

At the *physical level*, agents consider the properties (e.g., size), type (e.g., written) and source (e.g., transaction systems) of the sign. The information systems developer draws on these to design devices (e.g. transactional databases) for handling the data (i.e., the signs). A common problem at this stage is that, based on his/her experience, the inputs which the domain expert considers important may not be represented in the raw input data, or it may only be available in a way that the data mining tools can not recognize it (Apte *et al.*, 2002, Berry and Linoff, 1997).

At the *empiric level*, agents look at the statistical properties of the data objects. The information systems developer investigates the validity of the data, which is a function of its legitimacy and relevance. It is also necessary to pre-process the data in order to minimize some of the problems usually encountered in datasets. One problem is the existence of too many attributes that are, in effect, variant representation of the same data. Another problem is the incompatibility between different computer architectures which requires the data to be translated between platforms. Yet another problem is the inconsistency of data encoding and the possibility of missing data fields, such as questions not answered in a questionnaire or attributes not applicable to a given object. Finally, the datasets need to be cleansed of existing noise, such as random events that have no perceivable causality. Statisticians will, then, process the data according to the function to be performed by the datasets. Data will commonly follow one of six models: classification, estimation, prediction, clustering, summarization, or affinity grouping (Berry and Linoff, 1997, Fayyad *et al.*, 1996a, Fayyad *et al.*, 1996b, Jackson, 2002, Peacock, 1998).

At the *syntactical level*, agents look at rules for assembling complex signs from simple ones, structuring data items into meaningful steps, and linking them. Drawing on Peirce's work, the philosopher Charles Morris introduced the concept of 'semiosis', the process through which a knowing subject gives meaning to a sign (Morris, 1938/1970). Semiosis leads to the building of knowledge through abduction, deduction and induction. Abduction generates new ideas or hypotheses that explain

a given observation; deduction evaluates the hypotheses and draws logical consequences from the premises; and induction generates a rule based on a fact and conclusion (Staat, 1993, Yu, 1994). The rules are defined according to some grammar or code, for instance grammatical rules or mathematical formulae. The information systems developer may use one of the following approaches to developing syntactic analyses in databases: standard statistics, market basket analysis, memory-based reasoning (also known as example-based models), genetic algorithms, cluster detection, link analysis, decision trees and rules, and non-linear models (e.g. neural networks).

Social aspects of communication

Shannon's theory of information, however, does not have anything to say about meaning. It constructs the notion of 'significance' from statistical analysis, rather than semantics. A sign is "*everything* that, on the grounds of a previously established social convention, can be taken as *something standing for something else*" (Eco, 1976). When the boundaries of signs are clear and there is a shared consensus regarding the relationship between a sign and what it stands for, there is an unequivocal and logical mapping between any given sign and the reality. However, in most social cases, there is no such unequivocal relationship.

Semantics acknowledges the role of the context, or "social reality", in the formation of meaning. The semantic level helps us understand how agents interpret the information available in relation to the context. This is the opposite of "literal meaning", or the meaning that is independent of any context whatsoever (Searle, 1979). Literal meanings require unequivocal and logical mapping between any given sign and the object it refers to. However, as illustrated by (Winograd and Flores, 1987) and (Andersen, 1990), in most if not all social contexts, there is no such unequivocal relationship. The formation of meaning may also be influenced by time. The relationship between the sign and the object can have either static or dynamic components (Desouza and Hensgen, 2002). In the former, the occurrence has the same outcome regardless of time. In the later, the value of "information" declines with the passing of time between the moment data was collected and the moment the relationship was established.

The *pragmatic* level focuses on the role of the interpreter in establishing meaning. We consider the specific meanings of utterances and actions in use by actual speakers in concrete contexts (Searle *et al.*, 1980). Employees of a given organization, for instance, share a common culture and will tend to see the world in a similar way. These agents' common experiences have shaped their views and their assumptions (Liebenau and Backhouse, 1990). The common experience is comprised of formal and informal norms that guide the agents' actions within a community. Norms can be perceptual, cognitive, evaluative, behavioural and denotative. Agents within a given community use conventions and norms to guide their understanding of a sign. These reflect the tacit or formal agreement amongst the users about the appropriate uses of and responses to a sign. However, norms are non-deterministic in the sense that each agent will evaluate and select the norms that he/she considers relevant to the specific case, a selection that is naturally subjective. Nonetheless, norms have functions of directing, coordinating and controlling collective action and they correspond, at the social level, to the idea of an *affordance* at the individual agent level (Wright, 1963). Norms help individuals form expectations about the behaviour of others in social interactions. There are many sources of norms including religious, cultural, socio-political, coercive, business policies and employee codes. The information systems developer will refer to the norms to supply the rationale for actions taken by agents and the actions being modelled.

The communication acts, in turn, produce social consequences. For instance, the receiver of a message may be persuaded, confused, upset or amused. Additionally, obligations may be created, or discharged, as the result of exchange of information under given circumstances. Sales are agreed and partnerships are broken, for instance. The *social* level analyses the actual effects of the interpretation of signs by individuals (Stamper, 2001). It looks at the consequences of the communication process in the human affairs. These consequences are governed by social norms, which can be formal or informal, and explicit or implicit. The communication process may also have the effect of altering existing social norms.

The semiotic approach to the study of the communication process points to the conclusion that communication is accomplished only if the receiver understands both the message and the sender's intentions, and the social purposes are met (Liu, 2000).

Linking meaning with action – Application to the production and analysis of financial intelligence

The framework proposed in the previous section argues that the nature and context of signs, and their use, will impact on decision making.

Social researchers have shown that the creation and dissemination of meaning in an organizational setting is a process where subjectivity exists. March (1991), for instance, reports how the seemingly straightforward effort to model data in a telecommunications company about corporate real estate holdings faced extraordinary difficulties because each group within the organization had a different understanding of what constitutes a building, reflecting the conflicting ontologies to which the agents had to conform. For the accountants, a building was something that depreciates, whereas for the office planners a building was something that could be conceived as a contiguous space, to name just two different definitions (Marche, 1991).

The adoption of one specific interpretation has practical consequences for the agents involved as demonstrated by D'Cruz (2004). In her study of cases of child protection investigation, she describes how different interpretations of data emerge in different professional groups, how preferred versions of meaning override alternative ones, and what the consequences are for the parents and the children involved. Medical practitioners, social workers and police officers each have their own professional perspective that they bring to each investigation of suspected child maltreatment, often resulting in conflicting conclusions. Different meanings have different practical consequences for the children and their parents, ranging from income support to placement of the child in care (D'Cruz, 2004).

In the field of homeland security, Desouza and Hensgen (2002) use the semiotic framework to highlight the barriers to efficiency in the collection of information and to the effectiveness in the interpretation of that information prior to the terrorist attacks of September 11th 2001. The authors report that data related to the attacks had been reported to various intelligence centres since the beginning of 2001. Yet, the lack of understanding of any relational basis for this data (semantics), the underestimating of the intended actions of the terrorists (pragmatics) and the pursuit of independent paths by the agencies involved (social) seriously hindered the ability to develop a pre-emptive action plan (Desouza and Hensgen, 2002).

We now turn our attention to the field of anti money laundering and terrorism financing, and describe the application of the semiotic framework to the development of the identity of a criminal. The case described is part of a research project funded by the European Commission to develop a new technique for monitoring money laundering: the Behavioural Patterns Approach. The findings presented in this paper result from interviews with financial investigators operating in financial intelligence units and law enforcement agencies in Europe.

Background information

Terrorist organizations derive income from a variety of sources, often combining both lawful and unlawful funding, and where the agents involved do not always know the illegitimate end of that income. The forms of financing can be grouped in two types:

- a) *Financial support* – In the form of donations, community solicitation and other fundraising initiatives. Financial support may come from states and large organizations, or from individuals;
- b) *Revenue generating activities* - Income is often derived from criminal activities such as kidnapping, extortion, smuggling or fraud. Income may also be derived from legitimate economic activities such as diamond trading or real estate investment.

The terrorist financier will want to disguise the illegal end of the funds, while trying to maximize the revenues for the organization sponsored. It may be necessary to disguise the source of the funds, as well, either because such funds have an illegal origin, or because the organization wants to preserve the continuity of the legitimate financing. The need to camouflage the source and destiny of the funds means that terrorist financing has many overlaps, in methods, with money laundering. From the point of view of a financial investigator, there is a crucial difference between traditional money laundering and terrorist financing, however. The monitoring of financial transactions in traditional money laundering is done in order to link the funds to a criminal act that has taken place already and to strip the criminal and any accomplices from the economic benefits of engaging in criminal behaviour. In terrorist financing, however, the investigation is done in order to prevent individuals to gain access to

funds that could finance future criminal activity and, therefore, it is done in order to prevent a crime from happening. The monitoring of financial transactions with the purpose of identifying terrorist financiers, therefore, must take into account the intentions of those engaging in the financial transactions observed.

The task of identifying and reducing money laundering and terrorism financing activity lies, in most countries, with the Financial Intelligence Unit (FIU)³. The main tool to inform FIUs of potential money laundering and terrorism financing activities is the Suspicious Transactions Report (STR)⁴. The FIU analyses the reports received, builds an intelligence file, and forwards a number of cases for further investigation and eventually, prosecution by the competent law enforcement agency (LEA). This process is illustrated in figure 2⁵.

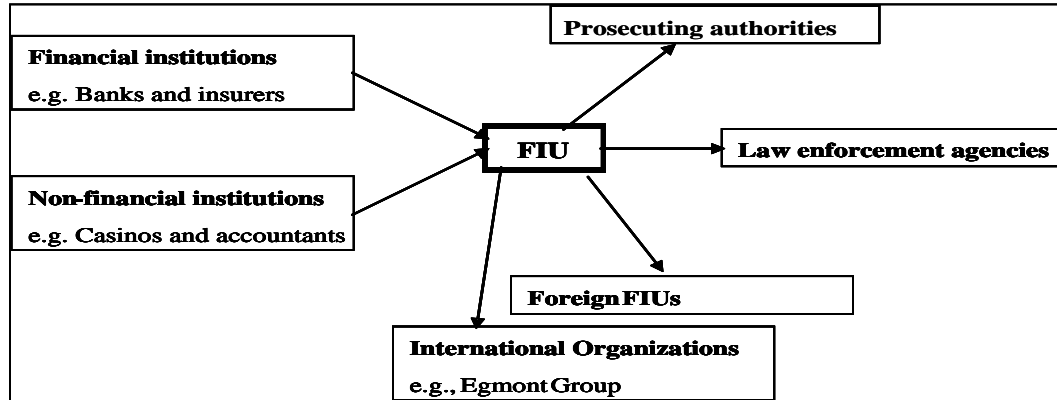


Fig. 2. Basic model of suspicious reporting in AML

The role of the financial investigator

The financial investigator operating in a FIU or LEA investigates individuals and organizations suspected of criminal activity (e.g., fraud or arms trafficking). The investigation is developed principally through the examination and analysis of the individual’s financial records, where necessary enhanced with data such as company registers, telephone registries, immigration and customs records, or vehicle registries.

The purpose of this investigation is to verify the legitimacy of the source and use of income and, possibly, to uncover the details of other individuals who may be involved in the laundering of any funds. In its daily activities, the financial investigator may interact with the individuals and organizations under investigation, as well as personnel of various local, national and international agencies, such as the local police forces, Inland Revenue or foreign FIUs. The investigator plays a key role in collecting, analysing and disseminating financial intelligence.

The trigger for a financial investigation is encapsulated in the following sentence from one of our interviewees: *“I am investigating [person A] because his legitimate income bears no resemblance to his lifestyle”*.

This apparently simple sentence raises quite profound questions that are at the heart of the success of the whole crime detection effort. For instance, issues regarding the definition of “legitimate” as well as regarding the expected relation between someone’s known source of income and the observed behaviour. Additionally, given that the financial investigator works in close collaboration with many other agents, in the case of any conflict whose definition or expectation should prevail? There is also an issue regarding the types of evidence – or signs – considered. Income may be an objective, measurable and to a certain extent verifiable entity, but how does one define, measure and above all verify the

³ Also known as “financial analysis unit” and “financial intelligence service”
⁴ Also known as Suspicious Activity Reports and Unusual Transactions Reports
⁵ Figure 2 describes a simplified version of the process of reporting suspicious criminal activity. In practice, the FIU also provides input (queries and information) to the reporting institutions, and it receives input from the other institutions identified in the figure.

lifestyles of, say, a plumber or a single parent? Lastly, who decides and how, when a subject falls in more than one category – e.g., a plumber who is also a single parent?

Technical aspects

Physical FIUs and LEAs collect and analyse data from STRs, reports of transactions related to terrorism financing, reports of transactions above a specified amount, reports of cross-border transportation of currency and bearer-negotiable instruments, as well as data from other FIUs (Gleason and Gottselig, 2004). Inputs include transactional data records such as financial products purchased by a given individual, and identification records such as the individual's known identities, addresses and professional occupation, among others. At this stage, the data collected is usually general, not necessarily collected for a single purpose.

Two main problems can occur at this stage that will limit the capacity of the financial investigator to assemble financial intelligence on a subject. One problem is that the data needed is not collected by the existing mechanisms. For instance, there is no data available regarding income derived from work done by subject A, as a plumber, in which no receipts were provided. While this may be a case of tax evasion, it is hardly a matter of concern for a drug squad.

The other possible problem is that although the data is available there are no schemes in place to channel it properly. This is the case with secrecy laws and limited sharing of information among agencies, in particular at an international level. While the travel patterns of subject A might suggest that he is smuggling goods into the country, there is no automatic transfer of data between customs and excise, and the financial investigator.

Empirics At this stage preliminary decisions are made regarding the data collected and the relative value of different sources of data. In establishing identity, for instance, the financial investigator needs to decide whether to consider official sources such as the electoral register, or commercial ones such as a utility bill.

A relevant factor for financial investigators is that the subjects under investigation tend to hold more than one financial product, often from different institutions. Each reporting institution will collect and report data regarding its own operations – for instance, savings accounts, life policies or mortgages held with bank X. However, for intelligence building purposes, it is necessary to look at all the financial transactions subject A performs in a given jurisdiction in order to have aggregated data at the individual level.

Investigators are also expected to update data regarding their subjects. However, that requires the cooperation of other institutions and agencies for an activity that is not necessarily justifiable by the day-to-day operations of that agency. Data from Inland Revenue can be very helpful in identifying assets acquired with illegitimate money – but if the individual under investigation is dead, there is no direct benefit for the Inland Revenue office, even though it is very useful for the work of the LEA. This update is also hindered by the fact that a large proportion of reports are still submitted in paper format – 50% in the UK, in 2004 - which significantly delays the processing of any useful information.

Syntactic At this stage, the analyst will search through the data available with the purpose of finding useful patterns of behaviour, or fitting an existing model to the data available to detect outliers. Failures at this stage are generally not about data collection but rather about putting data together. Financial investigators will generally use technical solutions to help uncover patterns. These solutions may have been developed for purposes other than anti money laundering – for instance, anti-fraud systems. Some solutions, however, were specifically developed for the detection of money laundering activity. These include standardised vendor solutions (e.g., I2 software) and *ad hoc* queries developed by in-house data miners (e.g., the loan sharking model developed by ABI, the banker's association in Italy). A common criticism levelled at data mining is that it is partly deterministic in the sense that analysts may only see what they are looking for (Humby *et al.*, 2003). Additionally, because data is not uniform, there is always the possibility that a sufficiently exhaustive search will suggest patterns that are simply the product of random fluctuations (Hand, 1998).

In financial intelligence specifically, this translates into focusing on the “usual suspects” and give more attention to anomalous activity coming from individuals with a given demographic profile. In one case, a personal assistant who stole nearly £4.5m over two years from her bosses, several suspicious

transaction reports were filed against the personal assistant, yet the case of her being a money launderer took some time to build because, in the words of a financial investigator interviewed by the authors, she “*did not fit the typical money launderer profile: man, white, 40 years old*”. Ironically, investigators were hindered by their very reliance on the “normal” profile.

The role of human behaviour at this stage is essential. Statistical know-how must go hand-in-hand with intuition and, even, creativity in order to identify the right patterns.

Social aspects

Semantics The financial investigator needs to put the relationships identified into context. First of all, the investigator must consider the legal context. The EU directive provides the common ground for all member states, but its transposition into national law has resulted in uneven applications. Some states have strengthened the requirements, while others have failed to implement it in full. There is also legislation that is specific to each member state, and that needs to be taken into consideration, as well. Recycling revenues from prostitution through the financial system is not considered to be money laundering in the Netherlands, for instance, where the activity is considered legal. Moreover, the reluctance of some jurisdictions to define “terrorism” creates even further discrepancies among the number and type of reports submitted to the FIUs and LEAs.

The subject-specific context also needs consideration, a practice usually referred to as “know your customer” (KYC). In one case, subject A was flagged by the system because of a sudden credit in his bank account. Further analysis quickly revealed that the peak was due to the sale of a house rather than the reward from a criminal activity.

Pragmatics The financial investigator needs to consider the intention of the provider of the information. The aim of the anti money laundering and terrorist financing system is to minimize the risk of not identifying and capturing the criminals. However, the regulatory instruments in place, such as the FATF’s blacklist or the imposition of heavy fines for failing to detect money-laundering activities, create a strong incentive for institutions to over-report. The incentives work such that for the reporting institutions it is better to minimize the error of false negatives, whereas for the FIUs and the LEAs it is better to minimize the error of false positives:

	Money Launderer	Honest citizen
Reported	Success	False positive error
Not reported	False negative error	Success

Additionally, the behaviour of the employee of the reporting institution is influenced by what is expected from him. A key set of norms to take into considerations is that regarding banking secrecy. Secrecy is a key differentiator for some segments of the financial industry, for instance. Indeed, the majority of the reports received by the financial investigators interviewed originate in the retail bank industry. Only a small percentage of the reports received originated from sectors with a strong tradition of secrecy such as private banking or lawyers.

The financial investigator is also aware that where there is no “safe harbour” provision, individuals incur a very heavy personal cost if they report suspicious activity. Therefore, the financial investigator tends not to get cooperation from individuals working in jurisdictions where there is no such provision.

There are also informal norms, both explicit or implicit, that bear significant weight in the quantity and type of information reported to the financial investigator. Our interviewees revealed that in Northern Ireland, for instance, a region with closely knit communities, there are important cultural barriers towards agents reporting certain terror-related behaviour.

Social Once behaviour is deemed suspicious, several obligations are created for both the financial investigator and the agency where he works. As a first step, the financial investigator must submit a report to a special commission, whose members decide on the best way to proceed in order to maximize the likelihood of a successful prosecution. The financial investigator is, in turn, obliged to follow the recommendations from this commission. The recommendations will include which agencies to contact in order to obtain further information. It will also refer which legal instruments to use in order to obtain proof of criminal behaviour that can be used by the prosecuting authorities – for

instance, the financial investigator may use court production orders, account monitoring orders and other instruments to obtain information of the transactions in a given account.

Once a complete intelligence file has been built, the investigator is obliged to contact the prosecuting authorities in order to try and bring this individual and/or organization to justice.

Discussion

The fight against money laundering and terrorist financing relies heavily on the capacity of financial intelligence units and law enforcement agencies to identify the criminals. The financial intelligence compiled and disseminated by financial investigators is of pivotal importance in the identification process and as an input for further investigation of potentially criminal behaviour. It is the investigator, whether aided by automated monitoring systems or not, who analyses patterns in transactional data and deems those patterns as suspicious.

The success of the fight against money laundering and terrorist financing is, therefore, influenced by both the efficiency and effectiveness of the process underlying the production of financial intelligence by the investigators. Because the investigator operates in an organizational context, it is necessary to understand the role of that context in the emergence of resulting classification.

Organization researchers have shown great interest in understanding how individuals interpret stimuli in the environment that surrounds them, and how these are reflected in the actions that such individuals take at the organizational level.

This paper looked at the duality, in an organizational context, between objective regulatory and technical categories, and the sense-making context of the financial investigation. Semiotics highlights how the process of the creation and use of information is shaped by and shapes the organizational environment.

Perceptions of social objects are naturally subjective and influenced by social referents. The construction of meaning in an organization setting is, inherently, a social process, and so the emerging category is socially constructed.

The framework proposed in this paper analyses information processing in six different steps, ranging from the technical to the social, and showing that communication is successful only when the receiver understands the message and the sender's intentions. The way agents generate, interpret and use information has key implications. The paper applies the framework to the specific case study of classification of the transactional behaviour as 'suspicious of money laundering or terrorist financing activities'. In this context, institutions must report their suspicions of criminal behaviour to the relevant authorities. The inadequate level and quality of reports submitted hinders anti-money laundering efforts. Under-reporting may mean that criminals are not being flagged. Over-reporting - a far more common scenario among FIUs - may mean that the LEA does not have capacity to analyse the reports in a timely fashion. A review of the reporting system in the UK, for instance, highlighted that as of mid 2003, the significant number of poor quality reports led to a backlog of nearly 60,000 STRs waiting to be analysed by the British FIU. Additionally, it revealed that the non fast-tracked STRs take on average 10 months before being sent to the law enforcement agencies, a delay that severely limits the agencies' ability to carry out successful investigations (KPMG, 2003).

STRs are considered one of the key variables in the subsequent number of prosecutions for money laundering activity (Bell, 2001), and an effective STR regime should lead to an increase in the amount of criminal assets recovered through use of STRs as well as an increase in convictions and other disruptions of criminal activity (KPMG, 2003). However, the proportion of processes sent for prosecution for laundering money or financing terrorism, over submissions of STRs is quite low. Data collected by the authors reveals that this proportion varies between 21% in Luxembourg and 4% in France, in 2002.

The process of producing financial intelligence, as discussed in this paper, is shaped by the social environment surrounding the individuals and organizations. The analysis, through the semiotic model, of the classification of subject A's behaviour reveals the technical and social inhibitors to efficiency and effectiveness in collecting, analysing and disseminating information regarding potential criminal activity.

Money laundering and terrorism financing is a criminal activity that, according to estimates of the International Monetary Fund, hides between two and five percent of the world's gross domestic product. Recent trends in anti money laundering strategy have focused on influencing the legal context and adopting technological solutions. These are the syntactic and semantic levels of the present framework. However, as discussed in this paper, the effectiveness of the anti money laundering and terrorism financing regime can only be enhanced if the remaining four levels of the semiotic framework proposed are also adequately analysed.

Conclusion

The performance of an information system is a function of its ability to generate, disseminate and use information. This ability is naturally affected by technical factors such as the information technology available in the organization. However, there is a growing recognition that social factors play a major role in the generation and assimilation of information. This paper introduced a way to examine information generation, dissemination and use that incorporates both the technical and the social levels in the organization, and specifically acknowledges the role of the decision maker.

The case study of classification of transactional behaviour, in the context of the fight against money laundering and terrorism financing, illustrated the role of the agent, technology and social context in constructing categories. Anti money laundering strategies have typically relied on technological and regulatory solutions. Instead, the focus needs to be more on social and pragmatic aspects of effectiveness in financial intelligence.

This paper aims to be an introduction to the use of semiotics in the understanding of categorization within an organization, in the field of crime prevention and detection. The present overview raises many issues of interest for future research.

Further research is needed regarding the agent in charge of deeming patterns as suspicious. Questions such as what makes a given investigator capable of deeming a given pattern as suspicious? Given the extreme interest in automated monitoring systems, it is also important to understand the role of automated monitoring systems in the classification process: Is the process driven by the knowledgeable investigator or, on the contrary, is it the software that drives the meaning?

The investigator does not operate in a vacuum. He/she will usually interact with others in the organization. In the case of different agents in the organization interpret the same pattern differently, whose interpretation prevails and why?

The paper stressed the role of formal and informal norms in the information interpretation process. Given that deeming a pattern as suspicious is a function of the prevailing norms, it is important to understand the relative weight of different norms, which norms prevail in case of conflicting directions, and what is the process by which the agent selects which norms to abide by.

The most critical task, however, is to link the subjective process of the decision maker with the technical and social aspects of information generation, dissemination and use. Such a link will help bridge the gap between the subjective cognitive process and the objective categories in use.

References

- Andersen, P. B. (1990) *A Theory of Computer Semiotics: Semiotic Approaches Construction and Assessment of Computer Systems*, Cambridge University Press, Cambridge.
- Annan, K. (2004) "Courage to Fulfil Our Responsibilities". in *The Economist*, 2 December 2004.
- Apte, C., B. Liu, E. P. D. Pednault and P. Smyth (2002) "Business Applications of Data Mining", *Communications of the ACM*, **45** (8), pp. 49-53.
- Austin, J. L. (1980) *How to Do Things with Words*, Oxford University Press, Oxford.
- Bell, R. E. (2001) "Discretion and Decision Making in Money Laundering Prosecutions", *Journal of Money Laundering Control*, **5** (1), pp. 42-51.
- Berry, M. J. A. and G. Linoff (1997) *Data Mining Techniques: For Marketing, Sales, and Customer Support*, Wiley, New York.
- Bisman, C. D. and D. Hardcastle (1999) *Integrating Research into Practice*, Wadsworth, Belmont, California.
- D'Cruz, H. (2004) "The Social Construction of Child Maltreatment: The Role of Medical Practitioners", *Journal of Social Work*, **4** (1), pp. 99-123.

- Desouza, K. C. and T. Hensgen (2002) "On "Information" in Organizations: An Emergent Information Theory and Semiotic Framework", *Emergence*, **4 (3)**, pp. 95-114.
- Eco, U. (1976) *A Theory of Semiotics*, Indiana University Press, Bloomington, IN.
- Fayyad, U., G. Piatetsky-Shapiro and P. Smyth (1996a) "From Data Mining to Knowledge Discovery in Databases", *AI magazine*, **17 (3)**, pp. 37-54.
- Fayyad, U., G. Piatetsky-Shapiro and P. Smyth (1996b) "The Kdd Process for Extracting Useful Knowledge from Volumes of Data", *Communications of the ACM*, **39 (11)**, pp. 27-34.
- Gleason, P. and G. Gottselig (Eds.) (2004) *Financial Intelligence Units - an Overview*, International Monetary Fund, Washington DC.
- Hand, D. J. (1998) "Data Mining: Statistics and More?" *The American Statistician*, **52 (2)**, pp. 112-118.
- Humby, C., T. Hunt and T. Phillips (2003) *Scoring Points: How Tesco Is Winning Customer Loyalty*, Kogan Page, London.
- Jackson, J. (2002) "Data Mining: A Conceptual Overview", *Communications of the Association for Information Systems*, **8** pp. 267-296.
- KPMG (2003) "Review of the Regime for Handling Suspicious Activity Reports" *KPMG LLP*, London.
- Levi, M. and D. S. Wall (2004) "Technologies, Security, and Privacy in the Post-9/11 European Information Society", *Journal of Law and Society*, **31 (2)**, pp. 194-220.
- Liebenau, J. and J. Backhouse (1990) *Understanding Information: An Introduction*, Macmillan, London.
- Liebenau, J. and G. Harindranath (2002) "Organizational Reconciliation and Its Implications for Organizational Decision Support Systems: A Semiotic Approach", *Decision Support Systems*, **33 (Issue 4)**, pp. 339-398.
- Liu, K. (2000) *Semiotics in Information Systems Engineering*, Cambridge University Press, Cambridge.
- Marche, S. (1991) "On What a Building Might Not Be - a Case Study", *International Journal of Information Management*, **11 (1)**, pp. 55-66.
- Morris, C. W. (1938/1970) *Foundations of the Theory of Signs*, Chicago University Press, Chicago.
- Peacock, P. R. (1998) "Data Mining in Marketing: Part1", *Marketing Management*, **6 (4)**, pp. 8-18.
- Peirce, C. S. (1931-58) *Collected Writings*, Harvard University Press, Cambridge, MA.
- Punch, K. (1998) *Introduction to Social Research*, Sage, London.
- Riessman, C. K. (Ed.) (1994) *Qualitative Studies in Social Work Research*, Sage, Thousand Oaks, California.
- Searle, J. (1969) *Speech Acts: An Essay in the Philosophy of Language*, Cambridge University Press, Cambridge.
- Searle, J. (1979) *Expression and Meaning: Studies in the Theory of Speech Acts*, Cambridge University Press, Cambridge.
- Searle, J., F. Kiefer and M. Bierwisch (Eds.) (1980) *Speech Act Theory and Pragmatics*, Reidel, Dordrecht, Holland.
- Shannon, C. E. and W. Weaver (1949) *The Mathematical Theory of Communication*, University of Illinois Press, Urbana, Illinois.
- Staat, W. (1993) "On Abduction, Deduction, Induction and the Categories", *Transactions of the Charles S Peirce Society*, **27** pp. 197-219.
- Stamper, R. (1973) *Information in Business and Administrative Systems*, John Wiley and Sons, New York.
- Stamper, R. (1993) "Social Norms in Requirement Analysis - an Outline of Measur" in *Requirements Engineering, Technical and Social Aspects*, (Jirotko, M., J. Goguen and M. Bickerton eds) Academic Press, New York.
- Stamper, R. (2001) "Organisation Semiotics: Informatics without the Computer?" in *Information, Organisation and Technology: Studies on Organisational Semiotics*, (Liu, K. ed.) Kluwer Academic Publisher, Boston, MA.
- Sturrock, J. (1986) *Structuralism*, Paladin, London.
- Winograd, T. and C. F. Flores (1987) *Understanding Computers and Cognition*, Addison-Wesley, Reading, Massachusetts.
- Wright, G. H. v. (1963) *Norms and Action - a Logical Enquiry*, Routledge and Kegan Paul, New York.
- Yu, C. H. (1994) "Abduction? Deduction? Induction? Is There a Logic of Exploratory Data Analysis?" in *Annual Meeting of American Educational Research Association*, New Orleans, Louisiana, April 1994,