2010

Detecting Money Laundering and Terrorism Financing Activity in Second Life and World of Warcraft

Angela S M Irwin
University of South Australia

Jill Slay
University of South Australia

DETECTING MONEY LAUNDERING AND TERRORISM FINANCING ACTIVITY IN SECOND LIFE AND WORLD OF WARCRAFT

Angela S M Irwin and Jill Slay

Forensic Computing Lab, Advanced Computing Research Centre
University of South Australia
Mawson Lakes, South Australia
Angela.Irwin@unisa.edu.au, Jill.Slay@unisa.edu.au

Abstract

In recent years there has been much debate about the risks posed by virtual environments. Concern is growing about the ease in which virtual worlds and virtual reality role-playing games such as Second Life and World of Warcraft can be used for economic crimes such as financially motivated cybercrime, money laundering and terrorism financing. Currently, virtual environments are not subject to the strict financial controls and reporting requirements of the real world, therefore, they offer an excellent opportunity for criminals and terrorism financers to carry out their illegal activities unhindered and with impunity. This paper demonstrates the need for suitable approaches, tools and techniques which can be used to detect money laundering and terrorism financing in virtual environments and introduces a research project which aims to establish a comprehensive set of behaviour maps, rule bases and models to help in the fight against organised crime and terrorism.

Keywords: Anti-money laundering, terrorism financing, counter terrorism, virtual environments, Second Life, World of Warcraft, massively multiplayer online role-playing game (MMORPG), massively multiplayer online game (MMOG), multi-user virtual environment (MUVE)

INTRODUCTION

As Internet technologies become more advanced, so have the ways in which terrorists utilise them for illicit and illegal activity. The Internet has become fertile ground for terrorists to obtain funds to support their operations (Rabasa *et al*, 2006) by participating in activities ranging from credit card theft using social engineering attacks such as phishing, hacking and keylogging attacks through to money laundering (Rabasa et al, 2006; Swartz, 2005). The ease with which terrorists have turned to virtual environments and information and communication technology (ICT), when traditional avenues of funding are restricted or lost, has become problematic for governments, counter-terrorism agencies and security professionals alike (Vallance, 2008; Nasir, 2009).

Al-Qaeda, the Taliban and other terrorist organisations have used money laundering for many years to conceal the identity, source and destination of legally and illegally obtained funds. Although estimating the amount of worldwide money laundering is challenging, the International Monetary Fund has estimated that between 2% and 5% of global GDP per year is generated annually as the proceeds of crime, that is an amount in the trillions of US$ (Asia/Pacific Group on Money Laundering, 2009).

Clear links exist between terrorism financing, money laundering, cybercrime and traditional criminal activity. Palmer (2005) quotes Mark Hunt of St. George's Bank who makes the connection between fraud, money laundering and terrorism financing when he states that "the lines between fraud and money laundering and terrorist financing are blurred, and they should not be treated as separate events. Nardo (2006) also makes the connection between criminal activity and terrorism financing. He states that "financial crime is a category which can generically encompass many others, like money laundering or terrorism financing or corruption or fraud. It has become clearer and clearer over time that all of these types show a certain degree of correspondence, and in a significant measure, interrelated and often connected in a wider common framework".

Although organised crime, cybercrime and financial fraud can and are being utilised by terrorist organisations, Hardouin (2009)) makes the important point that not all terrorism financing comes from illegal means; significant funds can be raised through legitimate businesses, fund raising efforts and donations. Equally, it must also be noted that money laundering and terrorism financing do not necessarily go hand-in-hand as a great

deal of money laundering activity is for private profiteering only and not for political purpose (Choo and Smith, 2008).

Following the money trail is a sound counter-terrorism tactic (Croissant and Barlow, 2007) in that the flow of money can help to identify donors, middlemen and recipient cells and their members. Although there is no concrete evidence to suggest that the lack of money puts terrorist groups out of business (Bergen, 2001; Bosworth-Davies, 2007), Nacos (2008) maintains that, "in order to support themselves, operate training facilities, acquire weapons, and travel, terrorists need substantial financial resources".

Investigating cybercrime involves recognising that a crime has taken place and finding out exactly what has happened (Mumford, 1999). This becomes very challenging when communications and funds are routed through a myriad of networks and people worldwide. In the case of financial crimes, the difficulty lies in being able to differentiate between legal and illegal activity. For example, when a terrorist carries out an illicit or illegal electronic funds transfer, it looks exactly the same as a lawful funds transfer. O'Connell (2008) asserts that why terrorists act in the way that they do is not as critical as knowing what they are capable of. Knowing this capability will help us to logically predict how, when and where to invest overstretched financial and human resources.

DEFINITION OF VIRTUAL ENVIRONMENTS

A virtual environment, also known as virtual reality, can be defined as a technology which allows a user to interact with a computer-simulated environment, whether that environment is a simulation of a real world entity or imaginary world. Most virtual reality environments are primarily visual experiences displayed on a computer screen but some simulations include additional sensory information such as sound. In 2009 it was estimated that approximately 600 million people worldwide were registered as users in virtual worlds (3D Perspective, 2009).

Virtual reality role playing games consist of three types: massively multiplayer online role-playing games (MMORPGs), massively multiplayer online games (MMOGs) and multi-user virtual environments (MUVEs).

MMORPGs take place in a continuous online world with hundreds or thousands of other players. Each player in the game controls an avatar which interacts with other players, carries out tasks to gain experience and collects items. Examples of the most popular MMORPGs are World of Warcraft, Lord of the Rings Online and Eve Online.

MMOGs are video games which are capable of supporting hundreds or thousands of players at the same time. MMOGs allow players to co-operate and compete with each other on a large scale, and sometimes to interact meaningfully with people around the world. They include a variety of game-play types such as flight simulation, government simulation and medieval fantasy. Examples of the most popular MMOGs are Rune Scape, Utopia and Domain of Heroes.

MUVEs refer to online, multi-user virtual environments, also known as virtual worlds. While the term MUVE has previously been used to refer to a generational change in multi-user dungeons (MUDs), Multiple User Dungeons, Object Oriented (MOOs), and MMORPGs, it is most widely used to describe MMOGs that are not necessarily game-specific. Modern MUVEs have 3D third-person graphics, are accessed over the Internet, allow for simultaneous user interaction, and represent a persistent virtual world. Examples of the most popular MUVEs are Second Life, Doom and EverQuest.

For the remainder of this paper the collective term of MMO is used when referring to MMORPGs, MMOGs and MUVEs. Although there are hundreds of MMOs available, the research project discussed later in this paper focuses on two, Second Life and World of Warcraft. The reason that these have been chosen is that they are the widely used, possess their own unique internal economies and have been highlighted by popular media as posing a significant money laundering and terrorism financing threat (Sanders, 2009; Sullivan, 2008; Tefft, 2007;).

Launched in 2003, Second Life was developed by Linden Labs. Second Life enables its users, called Residents, to explore and socialise with other individuals and groups. A major feature of Second Life is the ability for Residents to create and trade virtual property and services with one another.

The Second Life Software is a three-dimensional modelling tool based around simple geometric shapes which allow Residents to build virtual objects. The Linden Scripting Language can be used to add functionality to the

virtual objects created. External three-dimensional sculpted prim software can also be used to add textures to clothing, animation and gestures.

World of Warcraft (WOW), developed by Blizzard Entertainment, was launched in 1994. Using an Avatar, WOW players explore the landscape, fight monsters, complete quests and interact with other players. To enter WOW, the player must select a realm (or server). Each realm acts as an individual copy of the game world, and falls into one of four rule-set categories. Realms are either Player versus Player (PvP), where open combat among players is more common, or Player versus Environment (PvE), where the game-play is more focused on defeating monsters and completing quests; Role-Play (RP, RP-PVP) variants of both realm types are also available. Realms are also classified by language, with in-game support in the language available.

As characters become more developed, they gain a range of abilities and skills. Much of WOW play involves "questing". Quests generally reward the player with experience points, items, and/or in-game money. It is through quests that much of the game's story is told, both through the quest text and through scripted non player character actions. Quests commonly involve killing creatures, gathering a resources, finding difficult to locate objects, speaking to various non player characters, visiting specific locations, interacting with objects in-world, or delivering an item from one area to another.

THE RISKS POSED BY VIRTUAL ENVIRONMENTS

In recent years there has been much debate about the risks posed by virtual environments. Concern is growing about the ease in which MMOs such as Second Life, WOW and Entropia Universe can be used for economic crimes such as money laundering, fraud and terrorism financing (Tefft, 2007; Rijock, 2007; Sullivan, 2008; Methenitis, 2009; Sanders, 2009) and the potential and opportunity they offer for allowing large sums of money to be moved across national borders without restriction and with little risk of being detected (British Broadcasting Corporation News, 2008; Heeks, 2008; Leapman, 2007; Lee, 2005[A] & 2005[B]).

For example, the free-market economic structure and real-world value of virtual currency in some MMOs has blurred the boundaries between the virtual and the real. Initially, players were only able to convert virtual currency to real currency through the use of online auction sites. This changed to allow players to convert their digital earnings into real currency directly through the use of virtual currency arbitrage trading web sites. Convergence with the real world moved a step closer in May 2006 when Entropia Universe introduced real world ATM cards to its 250,000 players, allowing them to instantly withdraw hard cash from their virtual world assets (Entropia Universe, 2006).

Users can buy, sell, give and trade monies and goods by arranging for one Avatar to meet another to drop off goods or currency worth a significant amount of real currency. In so doing a digital transfer has taken place that has not been reported to any regulatory or investigative agency. The individual can then access the monies through the use of a MMOs ATM card. This is done quickly and easily, the receiver has clean money and no trail has been left behind.

Sanders (2009) provides a step by step guide as to how money laundering could be achieved using gold farming techniques (Figure 1). He also provides an example of how virtual gold can be transferred between real and virtual worlds and how this can be used to facilitate money laundering. In his example (Figure 2), the scenario is successful because there are a number of ways in which the money trail can potentially be lost.

Step 1	—›	Acquire a stolen credit card number.
Step 2	—›	Create a new account using a prepaid card on a MMOG with an active gold farming market, which allows both buying and selling of game currency. It is important that the virtual goods can be bought and sold.
Step 3	—›	Go to the gold farming sites and purchase the money with the stolen card and have it transferred to the new account.
Step 4	—›	Log on with a second account that has been purchased with a different credit card or prepaid gift card so both accounts are logged on at the same time.
Step 5	—›	Transfer the money from the first account to the second and then delete the first account.
Step 6	—›	Now sell the money to a place different from where it was purchased and have the proceeds transferred to a new bank account.

Figure 1: Gold farming, a step by step guide

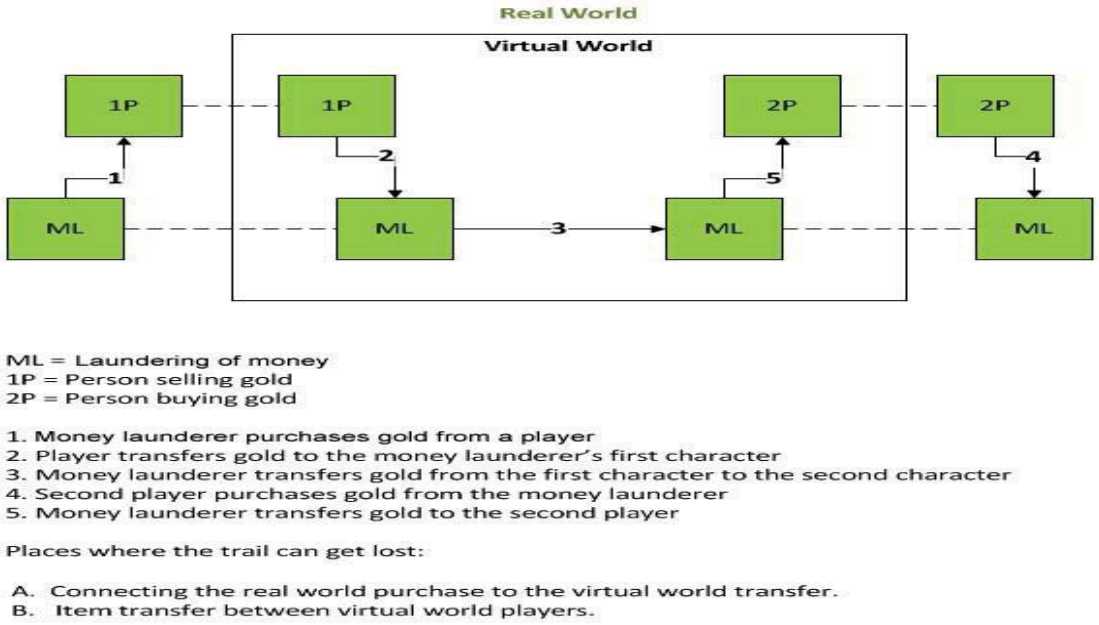

Figure 2: How the sale of virtual gold can be used to facilitate money laundering

The British Fraud Advisory Panel (FAP) identified the dangers of money laundering in Second Life and similar MMOs when they called on the British Government to extend real-world financial regulation into these environments. A study carried out for the FAP warned that criminal or terrorist gangs could transfer large sums of money across national borders without restriction and with little risk of being detected. In the report, Steven Phillipsohn, Chairman of the FAP's cybercrime working group, stated that "there is nothing virtual about online crime, it is all too real. It is time the government took it seriously". He goes on to say that Second Life is a "parallel universe with almost no external rule of law, no enforced banking regulations or compliance, no policing and no governmental oversight". A move to regulate Second Life would require the Government to extend the scope of watchdogs such as the Financial Services Authority (FSA), which oversees banks and financial markets in Britain (Leapman, 2007).

REAL-WORLD SOLUTIONS FOR VIRTUAL ENVIRONMENTS

Before the 2001 terror attacks on the United States, some countries, such as the Middle East and Africa, had no laws in place that criminalized money laundering and terrorism financing (FATF, 1999). The lack of effective anti-money laundering laws and regulations allowed terrorist financing to go unmonitored, as money transmitters were not required by law to register their transactions (FATF, 1999).

In recent years, however, considerable progress has been made in this area with the introduction of stronger anti-money laundering and counter-terrorism financing regimes and increased levels of inter-agency cooperation and support. This has enabled governments and law enforcement agencies to more effectively detect and prosecute money laundering and terrorism financing activities.

Money laundering and terrorism financing activities are traditionally detected, investigated and prosecuted through the proper implementation of strict financial transaction reporting procedures. These procedures aim to identify suspicious matters, unusual business dealings, use of placement techniques and international wire transfers of any value. Figure 3 shows the typical processes in place for detecting traditional money laundering and terrorism financing behaviour and demonstrates the how the current lack of controls and regulation can leave virtual money launderers and terrorism financers free to continue their activity unhindered.

Traditional ML & TF Detection	Virtual ML & TF Detection
Attempted placement/layering/ integration of illegally obtained funds into financial institution	Attempted placement/layering/ integration of illegally obtained funds into financial institution
Suspicions raised at financial institution	No controls in place
Suspicious Transaction Report sent to Financial Intelligence Unit (FIU)	No reporting procedures
Case investigated by FIU. If case to answer police and judicial authorities involved	No investigation undertaken
Individual charged/sentenced	Individual free to continue money laundering/terrorism financing activity

Figure 3: Processes in place for traditional and virtual money laundering and terrorism financing detection

Before controls, processes and procedures can be put in place to detect and counter virtual money laundering and terrorism financing, a number of important questions must be answered. These are: Can money laundering and terrorism financing activity be carried out in virtual environments such as Second Life and WOW? If yes, how can it be done? What constitutes suspicious behaviour inside Second Life and WOW? What makes a transaction suspicious? Is it an amount, an action or a series of actions? How can illegal and non-illegal transactions be differentiated? How can money laundering or terrorist financing be detected in Second Life and WOW when there are potentially millions of transactions per day, millions of individual account holders and no clear signature or pattern associated with money laundering and terrorism financing, especially when such activities can range from a single transaction to a culmination of months of complex transactional activity?

An important aspect of money laundering and terrorism financing detection is being able to identify the perpetrator(s), therefore, it is important to determine what personal information is collected from an account holder when an account is established within Second Life and WOW and ascertain whether this information can be associated with an individual in a real-world context. Also, can existing anti-money laundering and counter terrorism laws and Acts assist investigators in exposing the identity of account holders and the transactions they carry out in these environments?

In addition, can traditional, well-defined money laundering and terrorist financing behaviour models, detection procedures and frameworks be successfully applied to virtual environments? If not, what changes need to be made to make them suitable?

FOCUS OF RESEARCH

The main focus of this research is to identify money laundering and terrorism financing typologies and red flag indicators that may occur in virtual environments and create behaviour maps, models and suspicious activity rule bases for each of them. The research methods used to identify the money laundering and terrorism financing typologies and red flag indicators are document collection and analysis; in-depth, semi-structured interviews with key knowledge holders and subject matter experts, in-world observation and evaluation, in-world participation and model analysis and verification using Coloured Petri Nets.

A search was carried out to locate money laundering and terrorism financing typologies and case studies. As money laundering and terrorism financing typologies do not currently exist for virtual environments, typologies from the real world were used. A lot can be learned from real-world money laundering and terrorism financing, we can learn the motivations, the wide range of techniques used and the levels that individuals will go to to hide their illegal or illicit activity. It is the hypothesis of this research that many of the typologies found in real-world financial environments may be transferred to virtual financial environments.

For the purpose of this research, it was vital that the information analysed be from credible sources; therefore, information was obtained from a number of well-respected, international money laundering and terrorism financing agencies and authorities. These agencies and authorities contain experts with knowledge and a

thorough understanding of the pertinent issues and concerns related to money laundering and terrorism financing in their own jurisdiction and wider international community.

Information about potential money laundering and terrorism financing activity is collected from reporting entities through the submission of Suspicious Activity Reports (SARs). Reporting entities are required under law to submit a SAR for any suspected criminal conduct or suspicious activities that take place at or are perpetrated against their financial institution. When a SAR is completed, the reporting entity must provide a comprehensive account of the known or suspected violation of law or suspicious activity, including: who benefited, financially or otherwise, from the transaction, how much money was involved and how it was done. The reporting entity must detail any confessions, admissions, or explanations of the transaction provided by the suspect or any other person and indicate to whom and when the confession, admission or explanation was given (Elbanna, 2009). In addition, the SAR invites the reporting entity to determine whether it recommends any further investigation that might assist law enforcement authorities.

Suspicious Activity Reports are an excellent source of information and a valuable learning resource about current money laundering and terrorist financing activity and behaviour. Many anti-money laundering and terrorism financing agencies use the information contained within SARs and other reporting instruments to publish annual money laundering and terrorism financing typology reports, which are then communicated to Financial Intelligence Units (FIUs) worldwide.

Typologies are the study of methods, techniques and trends of money laundering and terrorism financing activities. Typologies assist anti-money laundering and terrorism financing experts and policy makers by providing them with up-to-date, empirical information and knowledge of the money laundering and terrorism financing environment, thereby allowing them to better target policies and combat threats.

By analysing typologies and case studies, a series of red flag indicators can be gathered. Red flag indicators are a set of circumstances that are atypical in nature or vary from normal activity and signal that something or someone may require further investigation. Red flag indicators help reporting entities to determine whether or not a suspicious transaction report should be submitted to their national FIU for further investigation. It must be noted that the presence of a red flag indicator does not imply illicit or illegal activity or guilt. However, in most cases the existence of multiple indicators raises a reporting entity's suspicion of potential criminal activity.

During the document collection and analysis phase, 500 real world money laundering and terrorism financing typologies were analysed. The typologies came from a number of sources, namely AUSTRAC, the Egmont Group, FATF, the Belgian Financial Intelligence Unit (CTIF CFI) and Moneyval, with dates ranging from 1996 to 2009. The purpose of analysing the typologies was to pull out the behaviours, also known as Red Flag Indicators, which were present in each case that initially cast suspicion that money laundering or terrorism financing was taking place.

Figure 4 below shows the next phases of research which will involve the grouping and classification of the typologies into 'Types', where they can be fully analysed in preparation for modelling. Patterns and behaviours associated with each Type will be collected, including entities, behaviours, red flag indicators and interactions between entities. Patterns will include all of the potential scenarios found in each Type.

Once each Type has been classified, government money laundering and terrorism financing key knowledge holders and experts will be asked to review and validate the results of the grouping and classification process to ensure that they are accurate and complete.

The next phase of research will be in-world observation and evaluation. During this phase it will be determined which of the real-world money laundering and terrorism financing Types can be carried out in Second Life and WOW. It is anticipated that an in-depth knowledge and understanding of Second Life and WOW will enable me to quickly and easily discount many of the Types collected and analysed in the previous step. During the in-world observation and analysis phase, it will also be established whether there are any additional money laundering and terrorism financing Types that have not been uncovered during analysis of the real-world money laundering and terrorism financing typologies because they are unique to Second Life and WOW.

In the in-world participation phase, there will be an attempt to replicate the Types deemed as possible in virtual environments. This will be done by creating the conditions necessary to carry out the behaviours and patterns identified for each Type – this will involve laundering money. It must be noted, however, that no money laundering or terrorism financing laws will be broken because to be classified as money laundering the money

must be illegal or illicit and turned into clean money. The money that will be used in this research will be clean, legal money.

To provide a scientific and measurable approach to the research, all of the money laundering and terrorism financing Types that are successfully replicated inside Second Life and WOW will be modelled using Coloured Petri Nets (CPNs). This will confirm the correctness of the Types identified and ensure that no assumptions have been made in the development of the behaviour maps, models and suspicious activity rule bases. During the modelling process, formal state space analysis will be carried out. The CPN models with capture the behaviour of entities and how they interact with each other. The state spaces generated will show all of the possible money laundering and terrorism financing scenarios for each Type.

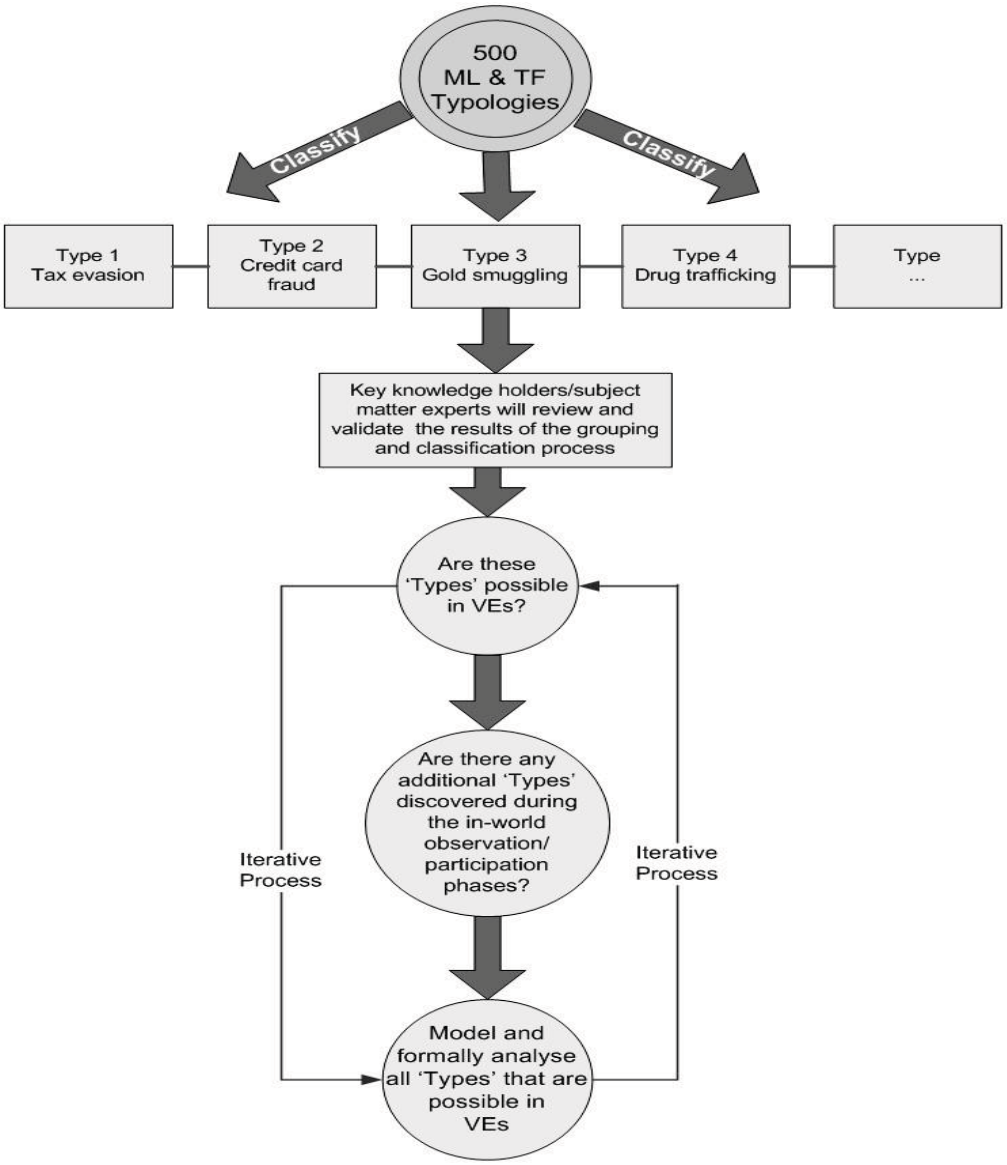

Figure 4: Process to be used to determine virtual money laundering and terrorism financing Types

CONCLUSION

The constantly evolving nature of money laundering and terrorism financing requires that opponent's strengths and weaknesses be constantly assessed at both technological and social levels as the degree of protection afforded to financial systems are merely temporary as investigators and anti-terrorism agencies continue to find themselves one step behind a constantly transforming adversary. The development of a practical typology, a strategic and tactical orientation, can guide homeland security professionals and investigators in identifying, assessing and defeating opponents.

Although real-world financial regulations do not currently extend to virtual environments, there is growing momentum for this to change. It can reasonably be assumed that, in time, virtual environments will be subject to the strict compliance laws and regulations faced by their real-world counterparts. Therefore, it is vital that pattern recognition techniques and suspicious behaviour maps, rule bases and models already be determined and systems designed to automatically detect potential money laundering and terrorist financing activities to ensure their transition into the virtual world is as smooth as possible.

REFERENCES

3D Perspectives (2009) Virtual World Concepts for CPG [www document] http://perspectives.3ds.com/2009/11/30/virtual-world-concepts-for-cpg/ (accessed: 17 December 2009)

Asia/Pacific Group on Money laundering (2009) Defining Money laundering: Scope and Nature of Problem [www document] http://www.apgml.org/about/history.aspx (accessed: 27 October 2009)

Australian Government Attorney-General's Department (2008) Counter-terrorism and related cases [www document] http://www.ag.gov.au/www/agd/agd.nsf/Page/Nationalsecurity_Counter-terrorismandrelatedcases (accessed: 1 October 2009)

Bergen, P (2001) The Bin Laden Trial: What did we learn? Studies in Conflict and Terrorism, Volume 24, Issue 6, pp 429 - 434

Bosworth-Davies, R (2007) Money laundering – chapter four, Journal of Money Laundering Control, Volume 10, Issue 1, pp 66 – 90

British Broadcasting Corporation (2001) US rocked by terror attacks, 11 September 2001, [www document] http://news.bbc.co.uk/2/hi/americas/1537469.stm (accessed: 28 October 2009)

British Broadcasting Corporation (2005) London rocked by terror attacks, 7 July 2005, [www document] http://news.bbc.co.uk/2/hi/4659093.stm (accessed: 28 October 2009)

British Broadcasting Corporation News (2008) Poor earning virtual gaming gold, 22 August 2008 [www document] http://news.bbc.co.uk/2/hi/7575902.stm (accessed: 21 October 2009)

Cho, K-K R & Smith, R G (2008) Criminal Exploitation of Online Systems by Organised Crime Groups, Springer Science, Asian Criminology, Vol. 3, pp 37 – 59

Croissant, A & Barlow, D (2007) Following the Money Trail: Terrorist Financing and Government Responses in Southeast Asia, Studies in Conflict and Terrorism, Volume 30, Issue 2, February 2007, pp 131 - 156

Elbana, M (2009) Using the U.S. Suspicious Activity Report (SAR) to Improve Reporting in the Middle East [www document] http://www.bankersacademy.com/pdf/SAR-middleeast.pdf (accessed: 23 October 2009)

Entropia Universe (2006) Entropia Universe Debuts First-Ever Real-World ATM Cards for Easy Access to Virtual Funds [www document] ftp://ftp.entropiauniverse.com/press_releases/PR_ATM_FINAL_5.2.pdf (accessed: 21 November 2009)

FATF (1998) 1997 – 1998 Report on Money Laundering Typologies, 12 February 1998 [www document] http://www.fincen.gov/news_room/rp/files/typo97en.html (accessed: 9 October 2009)

FATF-GAFI (1999) Report on Money Laundering Typologies 1998 - 1999 [www document] http://www.fatf-gafi.org/dataoecd/29/38/34038177.pdf (accessed: 16 June 2010)

FinCen (2007) 2007 National Money Laundering Strategy [www document] http://www.fincen.gov/news_room/rp/files/nmls_2007.pdf (accessed: 6 January 2010)

Gross, G (2010) Microsoft, eBay, Citizens Bank launch online fraud alert service, 17 June 2010, IDG News Service [www document] http://www.computerworld.com/s/article/9178193/Microsoft_eBay_Citizens_Bank_launch_online_fraud_alert_service (accessed: 1 July 2010)

Guardian (2008) Gunmen run amok in Mumbai terror attack killing and injuring hundreds, 27 November 2008 [www document] http://www.guardian.co.uk/world/2008/nov/27/india-terrorist-attacks-mumbai (accessed: 28 October 2009)

Heeks, R (2008) Current analysis and future research agenda on "gold farming": real-world production in developing countries for the virtual economies of online games, Centre for Development Informatics, University of Manchester, United Kingdom [www document] http://www.sed.manchester.ac.uk/idpm/research/publications/wp/di/documents/di_wp32.pdf (accessed: 19 October 2009)

ICC Commercial Crime Services (2007) Virtual money laundering threat identified, 12 November 2007 [www document] http://www.icc-ccs.org/index.php?option=com_content&view=article&id=144:virtual-money-laundering-threat-identified&catid=60:news&Itemid=51 (accessed: 12 October 2009)

Leapman, B (2007) Second Life world may be haven for terrorists [www document] http://www.telegraph.co.uk/news/uknews/1551423/Second-Life-world-may-be-haven-for-terrorists.html (accessed: 2 December 2009)

Lee J (2005[A]) From sweatshops to stateside corporations, some people are profiting off of MMO gold, 07 May 2005 [www document] http://www.erin-starr.com/From-sweatshops-to-stateside-corporations-some-people-are-profiting-off-of-MMO-gold.html (accessed: 10 October 2009)

Lee, J (2005[B]) Wage slaves, Computer Gaming World, July/August, 20-23 [www document] http://www.1up.com/do/feature?cId=3141815 (accessed: 20 October 2009)

Methenitis, M (2009) Virtual world money laundering, Law of the Game, 3 June 2009 [www document] http://lawofthegame.blogspot.com/2009/06/virtual-world-money laundering.html (accessed: 22 September 2009)

Mueller, R S (2006) The art of information, Vital Speeches of the Day, Volume 72, Number 14/15, pp 434 – 436

Mumford, E (1999) Dangerous Decisions: Problem Solving in Tomorrow's World, Kluwer Academic/Plenum Publishers, New York

Nacos, B L (2008) Terrorism and Counterterrorism: Understanding Threats and Responses in the Post-9/11 World, 2nd Edition, Pearson Education Inc, USA

Nardo, M (2006) Building synergies between theory and practice: Countering financial crime on a systemic approach, Journal of Financial Crime, Volume 13, Issue 3

Nasir, A (2009) The Taliban diversify into tobacco, 21 August 2009 [www document] http://www.thenational.ae/apps/pbcs.dll/article?AID=/20090822/FOREIGN/708219788/1135 (accessed: 24 September 2009)

Navias, M (2002) Finance Warfare as a Response to International Terrorism, The Political Quarterly, Issue 73, Volume , pp 57 – 79

O'Connell, P E (2008) The chess master's game: A model for incorporating local police agencies in the fight against global terrorism, Policing: An International Journal of Police Strategies & Management, Volume 31, Issue 3

Palmer, C (2005) A picture of terrorist financing, Counter Terrorist Financing, AML Newsletter, December 2005 [www document] http://www.amlmagazine.com.au/amlwr/_assets/main/lib7006/a%20picture%20of%20terrorist%20financing_issue2_december05.pdf (accessed: 3 July 2010)

Rabasa, A; Chalk, P; Cragin, K; Daly, S A; Gregg, H S; Karasik, T W; O'Brien, K A & Rosenau, W (2006) Beyond al-Qaeda: Part 1: The Global Jihadist Movement, RAND Corporation, Santa Montica, CA

Rijock, K (2007) China's central bank will regulate virtual currency, 13 January 2007 [www document] http://www.world-check.com/articles/2007/01/13/chinas-central-bank-will-regulate-virtual-currency/ (accessed: 22 September 2009)

Sanders, M (2009) Money laundering through gold framing and virtual goods, 3 June 2009 [www document] http://www.box.net/shared/nikjjgng3m (accessed: 22 September 2009)

Sullivan, K (2008) Virtual money laundering and fraud: Second Life and other online sites targeted by criminals, 3 April 2008 [www document] http://www.bankinfosecurity.com/articles.php?art_id=809 (accessed: 22 September 2009)

Swartz, J (2005) Terrorists' use of Internet spreads, USA Today, 20 February 2005 [www document] http://www.usatoday.com/money/industries/technology/2005-02-20-cyber-terror-usat_x.htm (accessed: 26 October 2009)

Tefft, B (2007) Will 5 new unregulated virtual banks become money laundering centres? 12 January 2007 [www document] http://www.world-check.com/articles/2007/01/11/will-5-new-unregulated-virtual-banks - become-money-/ (accessed: 22 September 2009)

Vallance, C (2008) US seeks terrorists in web worlds, BBC News, 3 March 2008 [www document] http://news.bbc.co.uk/2/hi/technology/7274377.stm (accessed: 26 October 2009)

Vande Walle, G (2008) A matrix approach to informal markets: towards a dynamic conceptualisation, International Journal of Social Economics, Volume 35, Issue 9

MAKING INFORMATION SECURITY ACCEPTABLE TO THE USER

Dr. Andrew Jones[1,2] and Dr. Thomas Martin[1]

[1]Khalifa University of Science Technology and Research
Sharjah, United Arab Emirates
[2] Edith Cowan University
andrew. jones@kustar.ac.ae

Abstract

The security of information that is processed and stored in Information and Communications Technology systems is an ongoing problem that, as yet, has not been satisfactorily resolved. Software developers, system architects and managers all aspire to use technology to provide improvements in the protection of information that is processed and stored on these systems. However, they are working in an environment where the threats to the information, the technologies in use and the uses to which the technologies are being employed are changing at a pace which is faster than can be effectively addressed.

This paper looks at the underlying environment of the technologies, social and economic change and the factors that affect how the end user perceives and interacts with the technologies.

Keywords: Information Security, Human Factors

INTRODUCTION

All organisations are facing the increasingly complex problem of securing their information and the systems that contain it. Information technology has become more useful and more useable, the initial capital costs and ongoing costs have dropped. All of this has lead to a greater dependence on ICT. In an effort to address the problem, an increasing number of legal and regulatory requirements have been introduced. Unfortunately these are, in many cases, almost unenforceable or pointless, as they have been brought into effect with a range of requirements to meet laws in individual countries and to meet perceived national and business sector specific requirements.

While work continues at many levels, experience of the past shows that to deliver international legal harmonisation of individual national laws takes a long time, it is set in an environment where the technology and the use and misuse that arises from it are changing rapidly.

The technologies that are being used, and in particular the Internet, are now almost ubiquitous and global and as a result there is inconsistency and confusion in the standards that should be applied to the protection of information. Security of information and information assets is not a problem that has only arisen with the increasing use of Information and Communications Technologies (ICT) to process, store and transmit information. As with many things in ICT, it is an old problem that has moved to a new environment. In the days before computers and mobile devices, sensitive information was stored in filing cabinets, safes and storage vaults. To protect this information, we relied on the vetting of staff, locks and bars and dedicated security staff that carried out periodic checks to ensure that the storage area had not been breached or if it had, then to report it within an acceptable period. As with any system that relies on human input, this was not foolproof and security breaches occurred on a regular basis with those that were detected being reported. Most of the reported security breaches were as the result of carelessness, accidents, theft or the illicit copying of documents. With the ever increasing use and complexity of ICT, the security of information has been addressed through the application of more and more technical solutions.

In part this is because the people that use the systems to carry out their roles within organisations for the most part only understand how to use the functionality of the ICT system that supports them in achieving their goals. Systems have been developed to meet the broadest possible consumer audience with the result that the unit cost has decreased significantly over time. ICT systems tend to be generic in nature and contain functionality that far exceeds the needs of most users. In the past, the tools that a person was provided with were the minimum that was required for them to carry out their role, for example a pen, pencil, paper, ruler, eraser (something to write with and make corrections with) or perhaps a typewriter. Now, with almost any ICT system, they will be provided with a suite of office tools (Word processor, spreadsheet, database system, presentation software) and