MIDLANDS FRAUD FORUM
Bringing the public & private sectors together

Cybercrime Research in Relation to Fraud, Economic Crime and Financial Crime

The **Midlands Fraud Forum** has commissioned this work using students from the University of Derby.

The aim of the project is to engage a student on a short-term basis to conduct a literature review for the benefit of the MFF (and its members via the MFF website) on the topic appropriate to a specific Master Class in connection with fraud and/or financial/economic crime.

This should provide MFF Members with an additional benefit and resource as well as give the students and opportunity to interact with the members attending the Master Class and to give them an opportunity to make a brief presentation.

As members make use of the research would you please be aware that:

Due to copyright restrictions, it is not possible to provide direct access to all copies of the underlying journal articles unless the publisher has made it openly available online. Readers may consult the embedded links in the annotated bibliography to see what access has been provided by the publishers' for each work. Direct online purchase is often the most expensive access method, so do consult your local library services which may be able to obtain access at cheaper rates or under subscription. You can also enter the title of a given article into an online search, many academics publish working paper drafts or sometimes pre-publication proofs for free access on their academic webpages.

MFF would be interested to have your feedback on this initiative; please email any comments to info@midlandsfraudforum.co.uk

We hope that you find it useful.

Executive Summary:

Cybercrime Research in Relation to Fraud, Economic Crime and Financial Crime

The aim of this project was to engage one or two undergraduate students to conduct a literature review for the benefit of the Midlands Fraud Forum (MFF). The topic area of cybercrime was defined broadly but in connection with fraud/financial/economic crime to foster relevance for the membership.

Practitioners are often very engaged in the business of moving from one operation to the next. Many may not be aware of literature on selected topics associated with their interests. Awareness and engagement with academic research may be even more difficult for the practitioner audience given chronic time management issues to identify, retrieve and read appropriate works.

This document provides an entrée into current academic literature on cybercrime issues and was generated through the following steps:

- A broad trawl through various open source and academic databases that generated nearly one hundred pages of potential references
- Sifting of materials to select those most connected to the core topic(s)
- Drafting of an annotated bibliography with a focused review for each of the entries included in the final sample
- Writing an executive summary to address key themes expressed from the reviewed literature
- Presenting the findings to an MFF masterclass on cybercrime and having the results published to the MFF website for the benefit of its members.

This summary highlights the key questions, themes and issues that emerged in the production of the annotated bibliography (appended below). Due to copyright restrictions, it is not possible to provide access to copies of the underlying articles. Each article is properly referenced using the Harvard system, and readers should therefore be able to obtain copies from their local library services, via online purchase or in some cases open internet access.

The first theme that emerges is the problem of the definition of the concept of cybercrime. In the absence of a standardised definition at the national or international level, the concept becomes embedded in over-broad legal definitions that cannot keep pace with the emerging examples and adaptations as technology progresses (Bronk et al., 2012; Collins & McCombie, 2012; Lusthaus, 2013; Stokes, 2012; Wall 2013b).

Where does fraud/economic crime begin and end as cybercrime, is this solely based on the use of technology and can victims or authorities reliably draw this line?

This leads on to the problem of appropriate measurement of cybercrime. It is troubling that data quality problems continue to impede our understanding. This applies to impact as well as the lack of reliability of the reporting infrastructure, which

hampers the development of information sharing partnerships and intelligence-led mechanisms to control cybercrimes (Williams & Levi, 2012).

What is the social organisation of cybercrime?

There has been surprisingly little effort to understand the social organisation of cybercrime. Perhaps there is an implicit assumption that it is very structured and systematic. There are some interesting parallels between cybercrime and organised crime. These are evident in the formation of significant co-offending networks and markets that facilitate the trade in illegal goods and stolen data where hierarchies and governance mechanisms of social control are in place (Hutchings, 2014; Hutchings & Holt 2014; Holt, 2013; Lusthaus, 2012; Yip et al., 2013).

The organised crime comparison is strained thought as exclusion is often the most serious penalty, given the difficulties in exercising direct control or violence against participants in often virtual settings. The distributed network model of terrorism may be a closer fit, where advertisement and internet chat room posts are used to solicit funds for terrorist financing (Bensted, 2012). Nevertheless, the scope of financial opportunity should imply the social organisation of cybercrime is variable and diffuse according to the nature of particular activities and the actors involved.

Which types of cybercrime are the biggest risk and threat to the UK and the international community? How should risk and threat be evaluated and compared across the known and emerging forms of cybercrime?

According to a sample from the UK information assurance (UKIA) network, the highest ranked cybercrime problems in the UK were personal identity theft and malware attacks, with denial of service attacks deemed to be causing the least problems (Levi & Williams, 2013). In an increasingly inter-connected and multi-layered world of social interaction, there are many bits of individual identity and data that may be vulnerable to identity theft. This may arise through the commonly-known method of ‘phishing’ (enticing people to share access to key financial or valuable social data), and the adaptation of ‘smishing’ which extends the technique from email and social media into the domain of SMS text messaging (Wall, 2013b).

Some point to counterfeiting and piracy markets (Guarnieri & Przyswa, 2013; Holt & Bossler, 2014) as the largest category by volume, with estimates that perhaps as much as 95% of films in the North American market are pirated. This is a problem affecting many regions where it has become common for many to simply download counterfeit video and audio, which is reinforced through peer to peer sharing and behavioural support, and corporate targeting of ‘anonymous’ users is deemed to be socially unacceptable in many jurisdictions.

Others point to the (expanding) issue of insider threats, which can range from malicious intent to negligence in the external sharing or damage of valued data. This can be much more severe than external attacks. Organisations report that more than forty per cent experienced an insider incident in the last twelve months, and surveyed office workers acknowledge their engagement in risky behaviour with corporate data on unprotected media (Wall, 2013a). There has been some research that suggests a movement away from offender profiling could be beneficial, and that

new detection signals may potentially emerge from the application of addiction theory to understanding insider threat risks (Maasberg & Beebe, 2014).

Another camp would focus attention onto a variety of technological advances that may signal a transformation in risk and threat. For instance, examples of malware such as the Stuxnet worm demonstrated that even complex network defences can be vulnerable to attack and manipulation for fraudulent activity, cyber terrorism, and state-sponsored cyber warfare (Collins & McCombie, 2012). The potential generation of hybrid criminal networks, via Botnets that command networks of infected computers, could significantly enhance both the intention and capability of cybercriminals beyond their traditional scope (Wagen & Pieters, 2015).

There is the widespread emergence of new payment and money transfer systems, which may be largely invisible to traditional fraud and laundering detection systems given high transaction volume and relatively small amounts (Bronk et al., 2012). Virtual currencies such as bitcoin, the linden dollar, and others are becoming increasing popular. These present laundering risks that are difficult to address in traditional detection systems that involve a focus on physical currency or transactions linked to traditional regulated banking and financial sectors.

There are other researchers who would emphasise the social aspects of cybercrime and fraud, perhaps most notably in the obscure area of studies into the romance scam (Buchanan & Witty, 2014; Whitty, 2013). The individual financial losses can range from £50 to £800,000 in a given case, but it tends to cause high distress levels to the victims regardless of the financial losses. Some personality traits may represent higher risk for victimisation such as loneliness, introversion and those who seek sensations via physical, social and financial risks. Ultimately, the scammer persuasive techniques model used by the offenders offers a systematic process to exploit and overcome victim defences. These include an idealised profile, grooming, and the sting request for money, and can include sexual or other forms of abuse, and expansion of the cycle of victimisation.

What does criminology research have to offer in addressing the problem of fraudulent or economically-motivated cybercrime?

Routine activity theory (RAT) advances the accessible model that crime occurs where motivated offenders and suitable targets (victims) interact in the absence of capable guardians (Williams, 2015). Despite the assumption of complexity and multiple jurisdictions, perhaps up to one third of fraudulent cybercrime may involve offenders and victims living in the same state/county (Bossler & Holt, 2012). There may be greater access to resources or training for national and international enforcement agencies. However, it should be clear that the asymmetry between criminal capability and law enforcement should result in greater attention to diffusing relevant aspect of cybercrime investigative skills downwards to the local level (Hunton, 2012; Guitton, 2013) and integration upwards to the national and international level (Button, 2012).

The capable guardianship approach also extends to enforcement efforts aimed at undermining the trust in networks for economically-motivated cybercrime. This could apply in several instances, and most clearly in the forums and markets for stolen

financial and other data (Hutchings, 2014; Hutchings & Holt 2014; Holt, 2013; Lusthaus, 2012; Yip et al., 2013). In undermining trust amongst criminal networks, law enforcement can increase the transaction costs for criminals who must balance risk of detection against the need to be accessible to their clients and availability to target their victims.

The routine activity model can assist in the realisation that the fear of cybercrime may hold similar or greater significance than cybercrime itself. For instance, fear of cyber identity theft and fraud has been shown to correlate with access and internet activity, but it seems that fear of traditional place-based crime is an underpinning factor (Roberts et al., 2013).

It does seem that there is a clear need to bridge the police-community gap and generate public confidence in capable guardians, which is, policing in the real and virtual world that better manages public knowledge and expectations as to the nature of the problems and the potential solutions (Bossler & Holt, 2012). This can assist suitable targets (victims) towards greater awareness of the role of the public in passive and active capable guardianship to protect themselves against the risk and threat of economically-motivated cybercrime (Williams, 2015).

Authors: Ms Emma Alexander and Mr Rowan Fogg
Final Year, Applied Criminology Programme

Supported by: Dr David Hicks d.hicks@derby.ac.uk
Department of Law and Criminology
College of Law, Humanities and Social Sciences
University of Derby

Annotated Bibliography:

Cybercrime Research in Relation to Fraud, Economic Crime and Financial Crime

Bensted, G. (2012). Hi terrorist financing and the internet: dot com danger. *Information & Communications Technology Law.* 21(3): 237-256. http://dx.doi.org/10.1080/13600834.2012.744222

Counter terrorism measures post 9/11 displays an emphasis in the prevention of fraudulent activities, specifically money laundering under US jurisdiction, resulting in the PATRIOT Act 2001 (Providing Appropriate Tools Required to Intercept and Obstruct Terrorism).

Terrorism is a worldwide threat and this article compares cross culturally legislative measures and preventions from the US, UK and the UN prior to 9/11. Terrorist financing within the US is most prevalent through the medium of advertisement and posting in internet chat rooms to solicit funds. Similarly to the US, the UK also has also seen a direct solicitation of donations via the same methods. However, prior to 9/11 the UK had legislation, Terrorism Act 2000, making terrorist financing an illegal act, opposed to the PATRIOT Act making an introduction post 9/11.

Prevention of terrorist financing may encounter certain difficulties due to the multi-jurisdictional structure the internet encompasses. The main difficulty will be global coordination due to the differing regulations within varying jurisdictions. However to combat this issue the UN created its Counter-Terrorism Strategy in 2006, to tackle the issue of global coordination. This will be done by Working Groups at an international and regional level identifying potential terrorist financing on the internet.

Bossler, A. M., and Holt, T. J. (2012). Patrol officers' perceived role in responding to cybercrime. *Policing: An International Journal of Police Strategies & Management.* 35(1): 165-181. http://dx.doi.org/10.1108/13639511211215504

The economic impact of cybercrime continues to put a strain on government budgets with the Government Accountability Office (GAO) estimating cybercrime costs the US economy $117.5 billion per year. Therefore the study seeks understanding into how local law enforcement responds to cybercrime and aims to improve the social response to cybercrime. The findings suggest officers do not believe local law enforcement should be responsible for cybercrime cases due to a lack of knowledge in the area. Which then in turn poses the issue of who to pass the crime onto if not local law enforcement? Despite participants deeming cybercrime to not be an issue for local law enforcement, between 20 and 35 percent of reports of fraudulent cybercrime have both the offender and victim living in the same state, meaning it is a local issue where contradicting jurisdictions are not an issue.

The study analysed a sample of two hundred and sixty-eight *(N=268) participants* with 86.4% of being male and 75.6% of white ethnicity. While not representative of the general population, these percentages closely relate to the demographics of the police forces that were surveyed. Results suggest practical implications would put the onus on the general public to protect themselves against cybercrime which would contradict the purpose of the study, improving social responses to cybercrime. Despite this, cyberspace is the largest social community meaning the traditional approach to criminal justice and bridging the gap between the police and communities may need to advance into cyberspace to instil public confidence in policing cybercrime. However, some patrol officers deem this ineffective because community partnerships are built over time and through interpersonal relationships.

Bronk, C., Monk, C., and Villasenor, J. (2012). The Dark Side of Cyber Finance. *Survival: Global Politics and Strategy.* 54(2): 129-142. http://dx.doi.org/10.1080/00396338.2012.672794

Technological advancements and the sophistication of systems offers new opportunities for cybercriminals to profit through money laundering. For example, accessibility to large quantities of networks and wireless devices does not benefit law enforcement to the same extent as criminals. This is due to enhancement in

opportunity to decentralise where the cybercrime has occurred leaving much untraceable in terms of time and cost for law enforcement.

Mobile money transfer (MMT) service providers seek to deploy systems and security to identify and combat money laundering. Movement of large sums of money via fewer electronic transactions may be easy to identify through traditional detection, however complexities occur when an online network generates a much higher level of transactions involving small monetary values and from what may appear to be randomly generated accounts. Furthermore, a high amount of transactions can add further complexities by the multiplicity of currencies, making detection more difficult. Despite this, the author does not offer any further solution towards prevention.

However, a clear framework for regulation is not prevalent for law enforcement agencies due to much legislation being drafted before the advent of social networking, peer to peer networks and the expansion of the internet. Therefore, modification of regulations needs to be updated to address the current financial environment cyberspace encompasses.

Buchanan, T., and Whitty, M. T. (2014). The online dating romance scam: causes and consequences of victimhood. *Psychology, Crime and Law.* 20(3): 261-283. http://dx.doi.org/10.1080/1068316X.2013.772180

The online dating romance scam is relatively new yet underreported, therefore an initial issue with prevention is the lack of experience to build upon in the practical world is limited. This scam can have significant financial and emotional implications on the victim, where fake profiles are set up and to build a relationship with a person with the aim to defraud them of large sums of money.

Scammers identify personality traits that pose high potential to handing over large sums of money. Traits include, loneliness, introversion and those who seek sensations via physical, social and financial risks. This study provides empirical research into identifying those who are most likely to be victims of this romance scam and the impact it has upon victims. Eight hundred and fifty-three online daters

(*N=853)* and three hundred and ninety-seven participants recruited from a victim support site (*N=397)* completed online questionnaires to measure the likelihood of falling victim to one of these scams. Analysis of the participants shows a wide range of personality traits and potential/previous victims creating a large group of potential victims. This may be due to the broad sample size, 369 men and 479 women with ages ranging from 19-81 partaking in the survey. Although 5 participants did not state their gender. The study does not discuss prevention techniques because of limited knowledge however does build upon the limited experience of law enforcement encounters with victims.

Results indicate high levels of distress irrespective of financial losses. The range of financial losses varies from £50 to £800,000 in a given case, however a significant correlation occurred where men and women differed in the severity of financial impact. This correlation being women suffered a significantly higher financial loss than men. However statistics into how much were not provided within the study. Despite this victims suggest the emotional impact vastly outweighs the financial losses. Furthermore, it is highlighted attention to how victims should be treated by law enforcement needs to be at the forefront because there is an argument victims of the romance scam are vulnerable/intimidated witnesses because of the psychological impact it may cause.

Button, M. (2012). Cross-border fraud and the case for an “Interfraud”. *Policing: An International Journal of Police Strategies & Management.* 35(2): 285-303. http://dx.doi.org/10.1108/13639511211230057

Understanding ever increasing issues of cross-border fraud, this study seeks to assess the structures that have emerged to tackle this issue. Furthermore, it aims to argue the case for an international body to help prevent cross-border fraud. The study focuses upon mass marketing frauds and phishing frauds because this has the widest impact in terms of number of victims and it does this by reviewing primary and secondary resources internationally to assess the methods to tackle cross-border fraud. However looking at structures that emerged nationally (UK) to tackle the problem of cross-border fraud is ineffective because it appears that the police

consider cross-border fraud as low priority. Nevertheless, national mechanisms for reporting economically-motivated cybercrime have been created which may encourage victim reporting. It also tackles the problematic misconception that if fraudulent activity occurs outside of the nation on a citizen of the UK, they can report it in their home country as opposed to where the crime actually occurred.

Weaknesses with current infrastructures are prevalent. EUROPOL, EUROJUST and OLAF were created to tackle problematic issues including cross-border fraud. EUROPOL is a European Union (EU) body established 1999 to co-ordinate the analysis and distribution of police information and intelligence. EUROJUST was established in 2001 to aid EUROPOL in investigating and prosecuting the most serious offences. OLAF is the European Anti-Fraud Office which focuses specifically on cross-border fraud. However, these infrastructures will only investigate where the financial benefit affects the EU. A further weakness is some jurisdictions require an eyewitness testimony to secure a prosecution. This method of operation is in the US. This can prove time consuming and stressful for witnesses who may potentially have to engage in significant travel to provide evidence.

With this in mind a case for a sole international structure may offer a solution to these weaknesses and prioritise cross-border fraud where some nations do not. This proposal would consist of an individual from each member state who would represent all concerns of fraud from that state. This proposal would differ from ones already present because this body has the primary focus of fraud opposed to other crime.

Collins, S., and McCombie, S. (2012). Stuxnet: the emergence of a new cyber weapon and its implications. *Journal of Policing, Intelligence and Counter Terrorism.* 7(1): 80-91. http://dx.doi.org/10.1080/18335330.2012.653198

Stuxnet is malware designed as cyber weapon to attack other computer systems. From this stems the potential for users of Stuxnet to benefit from further cybercrime such as fraud. The complexity of the Stuxnet malware can be used for fraudulent

activity, posing as a legitimate programme Stuxnet captures information incoming such as online banking details.

This article evaluates Stuxnet and the implications associated. This article also looks at how Stuxnet became a weapon for cyber-terrorists. It is highlighted an anti-virus company in Minsk, Belarus found the Stuxnet virus after their systems had become infected. Due to the complexity of Stuxnet, a worldwide alert was put in place despite the target of the malware was for a nuclear power plant in Iran. With systems infected, the aim of Stuxnet was to infect the control systems, causing the centrifuges in the uranium enrichment process to become uncontrollable thereby destroying them. This would have a large financial implication on the power plant and the targeted state. However, it is noted the financial implications from the destruction of the uranium centrifuges are much greater than the finances needed to create the Stuxnet malware.

The implications of Stuxnet disassembled the belief that the complexities of network defences would protect systems from cyber terrorism. However, the Stuxnet worm approach may have become for some governments a strategic tool that can a means of cyber warfare.

Guarnieri, F., and Przyswa, E. (2013). Counterfeiting and Cybercrime: Stakes and Challenges. *The Information Society: An International Journal.* 29(4): 219-226. http://dx.doi.org/10.1080/01972243.2013.792303

Counterfeiting serves an economic purpose for cybercriminals with experts estimating 80-95% of the market share in North America being pirated films. It is argued counterfeiting is not restricted to a national range but instead is a global phenomenon. This therefore adds to the complexities in preventative methods.

The internet plays a pivotal role within organized crime as networks decentralize the user enabling anonymity. This provides opportunity for crime such as counterfeit products. However due to the anonymity of the networks, understanding the infrastructure of organized counterfeiting cybercrime can prove difficult. With this in

mind, the authors argue the reason these organized crime groups are allowed to co-exist in cyberspace is fundamentally due to a lack of control within cyberspace. Furthering this argument, it is suggested counterfeiting in cyberspace is not a product of criminality but instead a result of capitalist society, therefore the prevention of counterfeiting becomes even more complex because society is immersed within capitalist ideology.

Guitton, C. (2013). Cyber insecurity as a national threat: overreaction from Germany, France and the UK?. *European Security.* 22(1): 21-35. http://dx.doi.org/10.1080/09662839.2012.749864

Gaining unauthorised access to government systems in separate incidents, hackers triggered panic amongst three nations, Germany, France and the UK. Publishing strategies to prevent a reoccurrence of unauthorised access, the threat of cyber security was evaluated.

The strategy of combatting the national threat in Germany focused on industrial control and data acquisition, protecting critical information. Since 2005 there was one other attack however the industrial control systems are yet to be under threat of another attack. Similarities between the three nations share the fear destructive attacks may be imminent in the critical infrastructure. However, the information being protected was different. The main concern for France was the lack of control on exchanged data however the UK sought to protect political and economic intelligence. The strategy within the UK expects businesses to induce transformations in the cyber security infrastructure however the article does not allude to why this is the strategy.

Holt, T. J., and Bossler, A. M. (2014). An Assessment of the Current State of Cybercrime Scholarship. *Deviant Behavior.* 35(1): 20-40. http://dx.doi.org/10.1080/01639625.2013.822209

Seeking gaps within the literature, the authors discuss cybercrime on a broad spectrum covering all aspects of cyber criminality. However, a common theme throughout suggests the motive for cybercrime is usually for financial gain or a financial impact on another. Piracy appears to be the most common form of cybercrime with theoretical underpinnings suggesting behaviour is learned from peers. However understanding the link between social learning theory and piracy makes the issue even more problematic due to the vast amounts of people committing the crime.

Ideas to prevent piracy have been considered such as infecting systems that try to download corrupt files. This may act as a deterrent however it may also be deemed unethical. The unethical approach this method adopts could potentially result in cyber warfare where members of the public try to fight off law enforcement agencies.

The financial gains and impact of piracy is a widely researched subject area, therefore this article proposes further research to be conducted in under examined areas such as fraud. This is because fraud is now operates in tandem with other forms of victimisation and can potentially affect large populations.

Holt, T. J. (2013). Exploring the social organisation and structure of stolen data markets. *Global Crime.* 14(2-3): 155-174. http://dx.doi.org/10.1080/17440572.2013.787925

As technology has expanded, an increase in people managing finances using the internet has increased. Parallel to this, a heightened risk has emerged as cyber criminals aim to utilise technology to commit fraud and financial theft from consumers. This article aims to apply a framework of social organisation to a sample of forums where financial information are bought and sold.

This framework posits that behaviour is focused towards an end goal. Social organisation entails three forms of behaviour: individual deviance, deviant exchanges, and deviant exploitation. Each form of transaction offers a different method of operation. Individual deviance requires a sole participant to commit fraud.

Exchanges requires collaborative work of two or more participants to complete the transaction. Finally, exploitation suggests the offender wishing to carry out the victim needs a suitable target.

The findings of the study parallel to the theory of social organisation suggest participants engaged in the sale of stolen data for financial gain. Deviant exchanges was the most common practice. This is because the illegal markets view participants as colleagues, and participants varying in deviant sophistication, the collegial environment enables participants to reach a specific goal more easily. However, the practicality of shutting down these forums may differ because of the varying sophistication of the markets. Also parallel with previous literature, issues with policy legitimising forums acts as an issue to law enforcement.

Hunton, P. (2012). Managing the technical resource capability of cybercrime investigation: a UK law enforcement perspective. *Public Money & Management.* 32(3): 225-232. http://dx.doi.org/10.1080/09540962.2012.676281

Multiple challenges are faced when investigating cases of cybercrime. This article seeks to unearth the difficulties law enforcement agencies encounter and how to maximise the efficiency and effectiveness of investigations.

Like any criminal investigation, cyber-investigations require knowledge and an extensive skillset. However, there is a distinct lack of resources in regards to global law enforcement in dealing with cybercrime as single entity. A lack of knowledge, training and awareness to the increasing threat of cybercrime has negative implications into responding to threat of cybercrime.

Focusing on UK law enforcement, much has been done to prevent cybercrime and improve the responsiveness of law enforcement agencies when dealing with cybercrime. The implementation of organisations such as the Serious Organised Crime Agency (SOCA) which was superseded in 2013 by the National Crime Agency (NCA) works alongside other police forces to combat the threat of cybercrime.

Further to public organisations, an increase in private organisations have helped public services in supplying security and aiding investigations via digital forensics.

Despite this, there is a distinct lack of discussion into the investigative process and how these agencies work alongside each other to reduce the threat of cybercrime. Furthermore, cybercrime is categorised as a single entity whereas for future discussion it may be more suitable to discuss a specific aspect of cybercrime. This is because methods of investigation would differ between types of cyber-criminality.

Hutchings, A., and Holt, T. J. (2014). A Crime Script Analysis of the Online Stolen Data Market. *British Journal of Criminology.* 54: 1-19. http://bjc.oxfordjournals.org/content/early/2014/12/29/bjc.azu106.abstract

A gap in literature identifies a limited understanding of economic situation of the online black market. This study sought thirteen (N=13) English and Russian speaking forums to formulate an understanding into what made offenders interact and engage within these market places. Therefore the aim of the study offers a practical aspect of prevention. The data used for this research are one thousand eight hundred and eighty-nine (N=1,889) exchanges between buyers and sellers from a sample of web forums where financial and personal information are bought, sold and traded. Ten of the forums were Russian speaking and three were English speaking forums.

Findings suggest specialist knowledge by offenders is obtained through free tutorials posted by other participants on the forum site. Specialist knowledge includes being able to discuss information regarding law enforcement so when transactions of payments and money laundering were to proceed, it would occur undetected. In turn this study highlights how offenders can target a large population (relatively) free of detection risk from law enforcement agencies. However law enforcement agencies do interact on the forums as a means of intelligence gathering and research.

Hutchings, A. (2014). Crime from the keyboard: organised cybercrime, co-offending, initiation and knowledge transmission. *Crime, Law and Social Change.* 62(1):1-20. http://link.springer.com/article/10.1007/s10611-014-9520-z

The key focus of this research looks at the relationship between co-offenders and fraud and how the internet facilitates organised crime and co-offending. Qualitative analysis views interviews from self-identified offenders and the law enforcement officers who investigate cases of fraud in regards to organised crime.

It is argued computer fraud does not occur online, however the internet can facilitate discussions on forums and organised crime can be initialised in these forums. Law enforcement agencies need to be aware that distractions are set up to cause panic that a cyber-attack is imminent, whereas the actual criminal activity will be taking place elsewhere.

A sample of fifty-four (*N=54) cases* was used in a qualitative research design to provide a further understanding of offending behaviour. The mean age of the sample was 30.6 years with 42 males and 12 female cases. Of the cases, 11 (20.4%) operated their fraudulent activity within a group of at least 3 offenders. The largest collaborative group consisted of 23 offenders. The second study interviewed fifteen (N=15) law enforcement officers *regarding* their experiences of investigating organised crime on the online markets. Eleven of the law enforcement officers believed offenders would work together as a way to distract and frustrate law enforcement as a means of hindering the investigation. However, this proved to be successful because law enforcement officers felt ill-equipped and the skillset of offenders vastly outweighed that of the officers, enabling offenders to commit fraud with relatively little risk of detection.

Offenders did not necessarily meet the definition of organised crime despite a sophisticated network of offenders cooperating to carry out an offence. This is because offending in this environment typically occurs in interaction with or through the influence of others. On the other hand, this study may be limited because the offenders who were interviewed were not selected at random and therefore may not represent the general offender population.

Levi, M., and Williams, M., L. (2013). Multi-agency partnerships in cybercrime reduction. *Information management and computer security*. 21(5): 420-443.

http://dx.doi.org/10.1108/IMCS-04-2013-0027

The authors designed this paper with the purpose of exploring and highlighting the multi-agency partnerships that are entrenched in the UK information assurance (UKIA) network. As public concerns grow, the lack of cooperation in cyber security is a problematic issue in the detection and reaction to cyber-attacks. A total of one hundred and four (N=104) surveyed members responded to the multi-dimension survey (MDS). The highest ranked cybercrime problem for the UK, as perceived by the sample from the UKIA, was personal identity theft and malware attacks, with denial of service attacks deemed to be causing the least problems.

Results indicated that there was over-crowding in cybersecurity space with insufficient knowledge of security needs and records to the successful prosecution of a cybercriminal limited therefore highlighting the existing gaps in public-private partnerships. To address the issue of cooperation amongst organisations, the gap between policing roles in the UK Cyber Security Strategy and various other policing roles needs to be bridged.

Lusthaus, J. (2013). How organised is organised cybercrime? *Global crime*. 14(1): 52-60.

http://dx.doi.org/10.1080/17440572.2012.759508

It has been recognised that the labels and umbrella terms applied to cybercriminals are often inadequately understood, a gap noted by this author aims to address through their attempt to provide answers surrounding the application of the definition of organised crime to cybercrime that is driven by profit. Previous studies have involved interviews with law enforcement agents, former hackers, internet security firm officers and the analysis of legal documents. However, they have failed to directly compare cybercrime and organised crime, something which this article focuses on.

Organised crime is referred to by the authors as a presence of governance embedded within the world of criminal activity with cybercrime concerned with the engagement of prohibited activity with the assistance and use of electronic devices or computers. Within the realm of cybercriminals, where hierarchies and specialist skill sets now exist, forums that operate in website form are platforms acting as a marketplace for illegal goods such as malware and stolen credit cards. The services of cybercriminals are also available for hire to carry out activities such as Denial of Service (DDoS) attacks. These forums operate with a form of governance where administrators offer a secure place for congregation. The presence of a police style role also exists with two principle aims, firstly providing reassurance to users of the safety of the site as a place for business and secondly acting as a deterrent to potential scammers.

However, forums and cybercriminals experience a short fall in obtaining the status of organised crime as although governance is present, it is weak existing only in the virtual sense where the most serious punishment is exclusion and therefore minor in comparison to the physical punishment carried out by organised crime groups. Forums are also a marketplace, another characteristic that is clearly not shared by physical organised crime. Smaller groups of cybercriminals demonstrate no formal hierarchy and will struggle to implement and maintain a form of governance. Cybercriminals experience challenges in being recognised as organised crime due to the absence and incapability of violence, and whilst DDoS attacks can be used as a method of control, physical violence cannot be achieved, something which is central to organised crime groups. Combined with the difficulties surrounding the existence and success of governance, it appears a traditional organised crime definition cannot be replicated in the virtual world.

Lusthaus, J. (2012). Trust in the world of cybercrime. *Global crime*. 13(2): 71-94.

http://dx.doi.org/10.1080/17440572.2012.674183

Anonymity of the internet provides cybercriminals with both opportunities and challenges, where they frequently encounter difficulties in the assessment of trust with potential business associates. It could therefore be assumed that cybercriminals operate independently; however, this should be avoided as they

frequently engage in partnerships. Given the transnational nature of cybercrime, studies encounter challenges due to the differences in jurisdiction and this study was therefore confined to the UK involving nine (N=9) interviews with members of law enforcement, hackers or cybercriminals and practitioners in internet security.

As the uncertainty of trust stems from the anonymity factor of the internet, criminals seek to find a balance which must enable them to be undetected by law enforcement but still remain visible enough to form potential partnerships. Three main mechanisms of establishing identity, assessing attributes and extra-legal governance exist to provide the fundamental framework for trust. One of the ways cybercriminals determine potential fake collaborators such as a law enforcement officer posing as a criminal is through the careful observation of behaviour patterns and language. Like many subcultures, cybercriminals have developed a unique version. However, it is recognised this is not the most successful mechanism.

It is considered almost impossible to arrive on the 'dark web' by mere coincidence as it requires dedication to remain relevant in the virtual world. Therefore cybercriminals often trust those who are online at the right time, based on the idea of selective environments, perceiving it as a signal that they are a committed cybercriminal. However, for law enforcement this could be used to their advantage as this mechanism of trust will not protect cybercriminals against an undercover officer who is able to dedicate their time to obtaining passwords to the dark web and establishing a presence. Law enforcement officers taking this approach should be aware of the tactics of background checks, evidence of criminal acts and information hostages to draw out undercover officers. This is a prime example demonstrating where anonymity can be both a benefit and a cost to cybercriminals. The demand for a user to display evidence of criminal acts is also used as a method to measure expertise or trustworthiness as opposed to identity. The presence of self-governance in an online forum also helps to build trust between cybercriminals because if a user is found to not be dependable by another cybercriminal, this will become known to the dark web community, potentially jeopardising future partnerships.

Maasberg, M., and Beebe, N., L. (2014). The enemy within the insider: Detecting the insider threat through addiction theory. *Journal of information privacy and security*. 10(2): 59-70.

http://dx.doi.org/10.1080/15536548.2014.924807

It is already known that insiders with malicious intentions pose challenges to security personnel as access to intimate organisational knowledge is often legitimate but can have detrimental financial implications to the organisations. The authors seek to move away from the behaviour profiling as the principle mechanism for detection and combatting of insider activity. They instead opt to focus on addiction, exploring the notion of addiction theory, a relationship alluded to in previous research but yet to be fully addressed. Although Carnegie Mellon Software Engineering Institute (SEI) Insider Threat Centre (known as CERT) exists as a detection process for fraud, the addiction theory discussed by this author many provoke an adaption of the stage of detection in currently adopted processes such as CERT. Exhibiting addiction does not necessary mean the individual becomes an insider threat, therefore this study seeks a construct that provides a correlation between the two components.

This author does recognise that the model remains untested, with privacy issues generating further challenges and limitations to research surrounding the addiction theory due to the minimised discussions of addiction in data concerning insider threats that is publicly accessible. Nevertheless, despite this and the need for empirical exploration into the detection signals, as the detection of an insider threat is frequently considered a greater risk and more challenging to eradicate than outsider threats, this study is useful in highlighting new detection signals that may help security personnel in future detection of insider threats.

Roberts, L. D., Indermaur, D., and Spiranovic, C. (2013). Fear of cyber-identity theft and related fraudulent activity. *Psychiatry, psychology and law*. 20(3): 315-328.

http://dx.doi.org/10.1080/13218719.2012.672275

The authors note the extension of traditional identity theft into cyber-identity theft and related fraudulent activity is a frequent topic within the media. Although attempted, research in this area encounters difficulties in providing an accurate determination of

the volume of identity theft and related fraudulent activity that is cyber related, predominantly due to the victims lack of awareness that they have been targeted for fraud or identity theft, but also their lack of awareness as to whether this was through an online or offline method. Therefore, the authors chose to explore the avenue examining the fear associated with cyber identity theft and related fraudulent activity. Involving a subset cohort of one thousand five hundred and fifty (N=1550) participants from the Australian Survey of Social Attitudes (AuSSA) conducted in 2007, the authors' thought that fear of cyber-identity theft and related fraudulent activity would be higher in those with higher income, that fear of place based crime will be significant as a predictor for fear of cyber-identity theft and related fraudulent activity, and finally that internet use will significantly predict fear.

Results generated from statistical tests did not show support for the principle hypothesis relating to higher income. The results also suggested that fear of traditional place based crime is a prominent driving force entrenched in the fear on cyber-identity theft and related fraudulent activity, supporting the second hypothesis and highlighting the potential of a generalised component regarding the fear of crime. It was also indicated that fear of cyber-identity theft and related fraudulent activity experiences a correlation with the level of access and internet activity. The authors noted the notion of 'exposure effect' applicable here whereby people who have heightened internet activity increase their chance of becoming a victim due to their regular use or through their frequent use they have developed a more comprehensive understanding of the current risks surrounding the internet and cyber-identity theft or related fraudulent activity, and therefore experience an increase in their level of fear.

Whilst various safety precautions can be practical mechanisms to reduce/prevent fraud the fear aspect cannot be eradicated as easily. Research surrounding the area of cyber-identity theft and related fraudulent activity is under researched and therefore, despite limitations highlighted by the author' this article still offers a much desired insight.

Stokes, R. (2012). Virtual money laundering: The case of Bitcoin and the Linden dollar. *Information and communications technology law*. 21(3): 221-236.

http://dx.doi.org/10.1080/13600834.2012.744225

This study highlights similarities with online gambling and suggests a method of incorporating linden dollars and bitcoins within the anti-money laundering framework. Due to extensions of global anti-money laundering regimes, money launderers are now required to exert some imagination into their practice. It is argued that much money laundering in the virtual world is achieved through the use of two currencies: bitcoins (the virtual currency which, through peer to peer software, allows for a transfer of value) and linden dollar currency (which is part of the online environment know as second life).

The evolution of money in the electronic form combined with the internet allows for potential cyber laundering, developed further into virtual laundering. The speed and ease of transactions give cybercriminals an advantage as they can now avoid limitations associated with physical currency. Both bitcoins and linden dollars would evade the current UK framework embodying anti-money laundering with law enforcements encountering difficulties in the detection of money laundering as a result of the capacity of legitimate transactions providing a concealment from which launderers are able to operate behind undetected.

The potential for money laundering risks is undoubtedly present with virtual currencies, and the current legal framework seems ill-equipped and would not suffice as an adequate instrument to deal with certain methods of transferring value.

Wagen, W., V., D. and Pieters, W. (2015). From cybercrime to cyborg crime: Botnets as hybrid criminal actor-networks. *British journal of criminology*. (In Press, Advance Online Access).

http://bjc.oxfordjournals.org/content/early/2015/03/06/bjc.azv009.abstract

The emergence of robotic like crimes dates back to various futurist predictions and this expectation is generating greater support with things such as networks of infected computers under the control of a ‘commander’, known as Botnets, having increasing importance in the role they play regarding a wide array of cybercrimes. As an entity that is neither in full human form nor solely driven by machine, Botnets pose a new type of challenge.

This study argues that the nature of Botnet style crimes cannot be understood if they are continually viewed as the human agency that commands them. Instead, a hybrid criminal network should be explored where humans and technology display mutual interaction and cooperation. In an attempt to explore this mutual interaction, the Actor-Network Theory (ANT) can be applied with the aim to promote the view that humans should not be prioritised and that the role of technologies and objects needs to be recognised.

To tackle Botnets, law enforcement must develop a comprehensive idea of the technological infrastructure. However, it is likely a cyborg structure will be needed in order to achieve a competent and successful defence against cyborg crime.

Wall, D., S. (2013a). Enemies within: Redefining the insider threat in organizational security policy. *Security journal*. 26(2): 107-124.

http://www.palgrave-journals.com/sj/journal/v26/n2/pdf/sj20121a.pdf

As electronic exchange of information has developed into the primary method of exchange, security provisions of most organisations are now constructed with the consideration of the threat that those on the inside can pose. This author examined empirical sources into the exploration of threats to organisations from insiders with consideration of the prevailing threat model and the creation of risk profiles of an insider. The insider threat is expanding with 43% of respondents to the Cyber Security Watch Survey (CSWS) conducted in 2011 expressing they had experienced an insider incident within the last twelve months. However, threats from insiders are not always with malicious intent. Some breaches of security can be a consequence of negligent and ill equipped insiders who skip security measures but do not breach data systems with malicious intent. A cross cultural study considered three thousand two hundred and fifty (N=3250) office workers across six countries and discovered 71% emailed work documents to home email addresses whilst 42% put work on USB sticks that were not protected. This highlights how insider threats can be non-malicious but occur as a result of negligence or their desire to meet performance goals. These insiders do not match the typical offender stereotype.

There are varying groups of non-malicious insiders, each posing different levels of risks to organisations. Some are prone to victimising themselves from malicious outsiders who target and persuade employees on lower incomes into sharing information. They may often act under the belief they are genuinely helping a customer for the good of the company. Data leakers may be inclined to share data they feel should already be in the public domain, predominantly through the use of social media platforms, and whilst depending on jurisdiction this can be an illegal act, it may not be malicious per se. Methods of data spillage can span from individual errors such as accidental disclosure through losing a memory stick and using public delivery services to send unsecure data or organisational errors including the failure to review user access rights.

Mechanisms to reduce these non-malicious threats from insiders will need to take various shapes encompassing numerous tactics. This could involve the redesign of security strategies to try and address lost data and data spillage. Organisation measures can also be taken in an attempt to reduce non-malicious insider threats. One option in this area is to review organisation goals and cultures as these are potential underlying causes of security breaches that involve goal and performance driven employees. If the organisation was to address the employee interpretation of the goals this would help to avoid any misinterpretation of the expectations placed upon employees and consequently could reduce threats to data security.

Wall, D., S. (2013b). Policing identity crimes. *Policing and society: An international journal of research and policing*. 23(4): 437-460.

http://dx.doi.org/10.1080/10439463.2013.780224

Identity related crime presents a threat to both individual citizens and the economy, with an estimated annual cost in the UK at £1.5 billion. The perception of identity related crimes are often differ from the reality, largely responsible for the emergence of challenges faced by police and consequently victim under-reporting and potential police over-reaction. This author explores the understanding of identity crimes, how they relate to traditional police practice and how some challenges have so far been addressed.

Police are becoming increasingly responsible for dealing with identity crime in an attempt to meet the demands placed upon them by the public, particularly with regards to the punishment of infringements involving social media platforms. However, they encounter difficulties regarding what protection the police are actually capable to deliver. Previous and more traditional methods of identity theft, obtaining personal documents that have been discarded, are increasingly replaced by the power of technology with personal information now being obtained through technological means such as phishing (where victims are tricked into revealing financial or related information through the use of emails or other common communication forms), a method that has since expanded into 'smishing' which adopts the same idea but using SMS text messages. As social media platforms expand, the gap between online and offline identities and identifiers is being bridged witnessing the emergence of new forms of identity such as social friendship, citizenship, financial, professional, organisational, and sexual and geographical affinities.

The principle challenge to police is the obligation they feel to respond to identity crimes, irrespective of the less visible profile, largely as a result of the pressure from the public. The author argues that UK legislation also creates a challenge as the law applicable to identity crime does not feature the terms identity crime or identity theft leading to the suggestion that they are concepts of a social rather than legal nature. Many people however are not calling for new UK legislation but instead seek better management of public expectations. This can be achieved through enriching public knowledge, enhancing the training undertaken by criminal justice agencies and further clarity of procedures. Clarity of responsibilities of the various public and private sectors would also address the apparent confusion between the state and citizen view regarding identity theft. The misreporting of identity theft from the public can have implications for the police such as the issue of overreaction. Surveys have alluded that the fear of cyber related crime is rife with a Scottish survey indicating that public fear was ten times greater than the experienced victimisation levels, offering a potential explanation to the perceived over-reaction of the police.

Whitty, M., T. (2013). The scammers persuasive techniques model: Development of a stage model to explain the online dating romance scam. *British journal of criminology*. 53(4): 665-684.

http://bjc.oxfordjournals.org/content/53/4/665.abstract

As the internet experiences an ever growing user base, the number of potential victims of persuasive techniques executed by criminals in the online dating romantic scam, stemming from paper based fraud and developed in 2007/2008, is also expanding. Victims are lulled into a false sense of security making them believe the false relationship formed through the online dating site is real before the criminal proceeds to ask the victim for money. This method could provide a substantial challenge for the policing of this type of cybercrime as the fraudulent activity may typically only cease when the victim comes to understand the true nature of the 'relationship'. As a relatively new approach used by criminals to target victims little is still known about the scam, therefore, this author recognised a noticeable gap in the research field and current literature. This study considers if the theories of persuasive techniques can be applied, offering a potential explanation as to why people are susceptible to victimisation of this scam.

To develop an understanding as to why people may become a victim of the online dating scam, twenty (N=20) participants both financial victims, with the amount of money lost ranging between £300 to £240,000 and non-financial victims took part in face to face interviews apart from one participant who resided in the US) discussing central themes to the scam. The results found that decision making errors associated with mass marketing fraud were similar to those of the online dating scam with the trusted person often adopting a fake persona of a position of authority. The research found that the victim also often made the decision to give money as they believed they were helping in a common scenario where people can struggle to resist the feeling of obligation such as paying medical bills for a sick child, and assumed their money would be repaid. Most participants expressed a feeling of addiction whereby even after discovering their victimisation, they struggled to break away from the 'relationship', potentially explaining repeat victimisation. An interesting finding in this study offering a potential explanation for repeat victimisation is the 'near-win' phenomenon often associated with gambling. Despite suspicions of

a scam the victim believes that if they send enough money they will eventually see some rewards.

The author provided the scammers persuasive techniques model, composed of seven stages, to enhance the understanding as to how and why people become victims. The seven stages consist of: motivation to find an ideal partner, being presented with an ideal profile, the grooming process (a carefully planned process demonstrating parallels to that of a sexual offender grooming a child) the sting where requests for money are made, continuation of the scam, sexual abuse (non-financial victims can be victims of sexual abuse through the use of webcams), and finally re-victimisation. This study offers an interesting and important insight into an under-researched area with results highlighting the importance of information and communication technologies as a platform in creating a trusting online relationship between victim and offender.

Williams, M. (2015). Guardians upon high: an application of routine activity theory to online identity theft in Europe at the country and individual level. *British journal of criminology* (Advance Access, In Press).

http://orca.cf.ac.uk/70423/1/Guardians%20Upon%20High.pdf

In Europe, online fraud is becoming one of, if not the most, prevalent crimes. Routine Activity Theory (RAT) is applied in this study to online fraud and the subset of online identity theft exploring country-level mechanisms. Social media platforms have experienced an increase in phishing attacks (the use of emails or other communication forms to trick victims into revealing personal and financial information) with 2.5 billion suitable targets exposed to motivated offenders of identity theft. Research indicates that compared to all other European countries, UK users are at a greater risk of victimisation with 250,000 phishing incidents in 2012. The application of RAT to cybercrime receives mixed results, although online identity theft and routine activity theory exhibit positive results.

Data collection was taken from the special Eurobarometer 390 survey on cybersecurity, with twenty six thousand, five hundred and ninety three (N=26,593) cross cultural respondents from twenty-seven countries. Results indicated that an

individual's routine activity theory is predictive of online identity theft. It was also concluded from results that passive physical guardianship, such as antivirus measures, act as prevention to becoming a victim of online identity theft and less security measures would increase the user's chance of victimisation. The findings suggested that active guardianship such as the individual user changing their passwords was likely to occur as a post victimisation action. Internet penetration was found to contribute to the occurrence of online identity theft, highlighting the need for infrastructure that is more secure.

Evidence of these working national cybercrime security strategies is vital to organisations and national government if they are set on dedicating substantial resources to the strategy development.

Williams, M., and Levi, M. (2012). Perceptions of the eCrime controllers: Modelling the influence of cooperation and data source factors. *Security journal (*Advance Online Publication).

http://www.palgrave-journals.com/sj/journal/vaop/ncurrent/abs/sj201247a.html

In regards to crimes that have an impact on the public, eCrime has now become a higher priority than traditional crimes (such as car theft and burglary) and is now a central component in the national security strategy of multiple countries with it being a Tier One threat in the UK. Despite its prominence, there remain disputes surrounding definitions and appropriate measurements, largely due to the roots of eCrime obviously embedded in technology.

Data involving eCrime and the impact on businesses, general public and national infrastructure are lacking in reliability hindering the understanding and development of controlling mechanisms of these crimes. Surveying eCrime using random probably approaches are responsible for the largest representative data, however, the reliability and validity is somewhat undermined as a result of issues concerning the terminology of survey questions. An increase in partnership and the sharing of information is sought after by the UK Cyber Security Strategy to assemble a tactical battle against eCrime that is driven by intelligence.

Yip, M., Webber, C., and Shadbolt, N. (2013). Trust among cybercriminals? Carding forums, uncertainty and implications for policing. *Policing and society*. 23(4): 516-539.

http://dx.doi.org/10.1080/10439463.2013.780227

The authors examine the structure of organised cybercrime and data from underground markets. In order to understand the cybercrime constructs that have emerged transaction cost economics (TCE), disorganised crime and social psychology were considered. As the UK has ranked cybercrime a Tier-One threat, with the USA and Australia executing comparable action, it is imperative that law enforcement have a coherent understanding of the way in which the current problem of cybercrime has manifested itself, with cybercriminals opting to use underground markets largely as a result of the hybrid organisation structure.

Analysis of real conversations in online underground markets, or carding forums, between cybercriminals was conducted to obtain an idea of how trust is obtained in the underground economy. It is thought that within the boundaries of trading in the underground market, carders face the greatest uncertainty concerning the identity of their follow collaborator, often fearful of trading with undercover law enforcement personnel, or the consideration of the quality of the goods.

Law enforcement have multiple avenues that require attention in the assistance of the reduction of cybercrime, particularly on carding forums. The principle area would be to prevent the development of trust between criminals on online platforms, as trust is fundamental to the underground market. This could be achieved through three means: Sybil attacks (increasing the number of undercover officers), increasing sentence length, and finally the removal of the carding forums. Arguably this should be the priority of the police because if the carding forums do not exist there is no arena for trust to be developed. Undercover officers should also dedicate time to practicing typical characteristics of a cybercriminal in an effort to prevent themselves from producing anomalies in their behaviour so as to avoid detection by cybercriminals.