International Digital Organization for Scientific Research ISSN: 2550-7974
IDOSR JOURNAL OF ARTS AND MANAGEMENT 3(1): 30-41, 2018.

Cybercrime and On-Line Safety in Cyberspace

Saja Bukhari
Department of Computer Science University of the Gambia

ABSTRACT

Cybercrime is essentially a transnational crime with a 'modus operandi' that exploits inter-state differences in the capacity to respond to such crime, and appears in the same company as such powerful global concerns as civil war, genocide and poverty. This transnational character provides cybercriminals, especially organized crime (OC), with the agility to avoid counter-measures even when implemented by capable actors. Although some have questioned the existence of organized criminal activities in cyberspace, several studies have noted the potential and actual synergy between organized crime and cyberspace in recent years. This paper outlines some of the issues and problems in respect to the role of OC in cybercrime.

Keywords; Cybercrime, transnational, crime, civil war, genocide and poverty.

INTRODUCTION

Information and communications technologies (ICT) have become a crucial element in our day-to-day activities; and lie at the heart of critical infrastructures around the world and key components, particularly in the technologically advanced countries [1, 2, 3]. This is hardly surprising as the proliferation of ICT and connectivity of the internet in today's information age open the door to increased productivity, faster communication capabilities, and immeasurable convenience [4]. Unfortunately, our increased dependence on ICT and the pervasive interconnectivity of our ICT infrastructure exposes us to an evolving spectrum of cyber-threats [5, 6]. Justice Sidambaram, District Judge of Singapore's Subordinate Courts, explained that [w]e live in a world of constant change [7]. Trade and technology interact to accelerate the rate of change [8]. Science and technology of today may become history tomorrow, while the knowledge and skills we acquire now may fast become obsolete. As a result, the current operations in an ever-changing environment are constantly faced with new challenges. With the arrival of the information age, complex crimes such as computer crimes, phone cloning and other high-technology crimes have emerged [8]. Cybercrime is essentially a transnational crime with a 'modus operandi' that exploits inter-state differences in the capacity to respond to such crime, and appears in the same company as such powerful global concerns as civil war, genocide and poverty (United Nations 2004 [9]. Although there is no definitive list of what constitutes cybercrime or computer related crime a consensus has emerged about what falls within the scope of the offences that occur in cyberspace [10]. 1. Telecommunications Theft & Illegal Interception 2. Piracy Copyright Theft 3. Cyber Stalking 4. Electronic money laundering and Tax evasion 5. Electronic Vandalism, Cyber-Terrorism, Denial of Service, Extortion 6. Sales and Investment Fraud, Forgery (Classic Pyramid schemes) 7. Electronic Funds Transfer Fraud and Counterfeiting (Carding, Identity Theft

and Misrepresentation) 8. Content Crime - Offensive Materials 9. Espionage 10. Resource Theft - illegal use of personal computers (PCs) or other digital devices [11]. Cybercrime ranges across a wide spectrum of activities and behaviors: at one end are crimes that involve fundamental breaches of personal or corporate privacy, such as assaults on the integrity of information held in digital depositories, identity theft and the use of illegally obtained digital information to blackmail a firm or individual. Midway along the spectrum are transaction-based crimes such as fraud, trafficking in child pornography, digital piracy, money laundering, and counterfeiting [12]. These are specific crimes with specific victims, but the offender hides in the relative anonymity provided by the Internet [13]. Another aspect of this type of crime involves those that deliberately alter data for either profit, personal or political objectives. At the other end of the spectrum are those crimes that involve attempts to disrupt the actual workings of the Internet. These include spamming, hacking, and denial of service attacks against specific sites to acts of cyber-terrorism by non-state actorsthat is, the use of the Internet to affect a nation's economic and technological infrastructure and cause public disorder or disturbances and even death [14, 15,16].

THE THREAT ENVIRONMENT

Cyberspace provides criminal actors a safe haven that enhances their organisational and operational capabilities [17, 18,19, 20]. Information security and associated laws and policy are also less well developed in emerging economies, thus providing an environment in which criminal activities can be conducted at lower risk but still have an impact on advanced economies [21]. Such threats are increasingly important and strategically relevant. For example, a 2008 report of the Centre for Strategic and International Studies (CSIS) Commission on Cybersecurity for the 44th Presidency began with a central finding: 'The United States must treat cyber-security as one of most important national security challenges it faces [22]. A 2009 Australian Defence white paper also voiced similar concerns. ICT advances have undeniably changed the way criminals conduct their activities, and policing also needs to adapt enforcement strategies that reflect changes in society. With the increasing digitalisation of information, 'policing will be carried out over a borderless community, rather than within the confines of national boundaries [23]. In response to the changing societal landscape, Grabosky explained new forms of policing, involving the harnessing of nongovernment resources, will become essential. Given the fact that cyberspace knows no boundaries, and that computer crime often transcends national frontiers, effective countermeasures will also require a degree of international co-operation which is without precedent [24].

DATA BREACHES

Almost every business in developed economies makes use of the internet. As businesses continue to engage in electronic commerce, they will become increasingly globalized and interconnected and the level of data being created by society is set to increase. In terms of the future threat landscape, it is argued that the increased variety and volume of attacks is inevitable given transnational crime networks' desire to obtain personal and confidential information [25]. Not all criminal misuse of computers or digital devices involves

hacking since passwords, PIN (personal identification numbers) and other protective codes can be obtained by 'social engineering'1 to gain access then erase, modify or copy the information to suit the needs of their attack [6]. Non-physical data breaches (e.g. due to computer or network intrusions) are a cause for concern. According to the data breach investigations conducted by Verizon Business from 2004 to 2008, for example, only 9% of the 90 data breaches (involving 285 million compromised records) were attributed to physical attacks. In the Verizon investigations, hacking is one of the leading causes of data breaches (64% of cases) and reportedly a favoured technique of cybercriminals, and 'unauthorised access via default, shared, or stolen credentials constituted more than a third of the entire Hacking category and over half of all compromised records [11]. The involvement of OC groups in computer or network intrusions such as hacking and unauthorised access to obtain sensitive information now emphasises the importance of large-scale profit-driven incentives. As noted by [14], a Senior Counsel with the United States Department of Justice's Computer Crime & Intellectual Property Section, 'compromise of credit and debit card account information most often results in the type of identity theft referred to as "account takeover," which involves fraud on existing financial accounts'. For example in a recent case in the United States, two accused persons were indicted on charges of "unlawfully, intentionally, and knowingly, acting in interstate and foreign commerce", via access of a computer and "thereby obtaining information from a protected computer for the purposes of commercial advantage and private financial gain". According to court documents, both accused persons (and others known and unknown) 'allegedly participated in a scheme to steal funds from bank and brokerage accounts by hacking into those accounts through the internet, using personal financial information obtained through computer viruses' (United States of America v Alexander Bobnev and Alexey Mineev2). The accused persons subsequently sent a portion of the stolen funds to their associates in Russia using money-remitting services after keeping a portion of the fraud proceeds for themselves [15].

INTERNET FRAUDS, SCAMS AND PHISHING

In online or internet scams, cybercriminals abuse the internet to reach out to potential victims across the globe by sending unsolicited messages purporting to originate from legitimate organisations in order to deceive individuals or organisations into disclosing their financial and/or personal identity information [4]. Information obtained from 'phishing' 3 and other illegal means is often for the purpose of using it to commit or facilitate crimes such as financial fraud and identity theft. A 2008 Gartner survey of 4,988 American adults, for example, indicated that top causes for financial fraud against consumers and payment card frauds are data breaches at a retailer, government agency or other, and third party 'phishing'[9]. The biennial KPMG fraud survey of 420 organisations in Australia and New Zealand reported similar findings. Within the financial services sector, credit card fraud accounted for 39 percent of the value of fraud attributable to external parties. Fraudulent access to financial services' accounts [by adopting the identity of the account holder by

'phishing' or 'Trojan horse' attacks over the internet] amounted to 31 percent of the total value attributable to external parties [17]. Several researchers and security practitioners have also suggested the involvement of OC groups in phishing scams and messages are increasingly targeting top company executives—also known as 'spear phishing' or 'whaling' in reference to bigger 'fish' [18]. OC groups have also been known to use identity fraud to either conceal their identities to evade detection and protect their assets from confiscation or as an enabler to commit various frauds and other crimes. Internet frauds and scams include 'advance fee' frauds (also known as '419' cases named after the relevant section of the Nigerian Criminal Code), online auction frauds, identity and payment card frauds. These take many forms but include, enticements to use your bank account to deposit the plunder of a former despot in Africa, administrative fees to transfer a huge lottery pay-out (for which you strangely cannot remember buying a ticket), or the bond money and advance rent for a non-existent but reasonably priced apartment suitable for an international student, and so on. Out of 275,284 complaints to the Internet Crime Complaint Centre in 2008, 26.5% or 72,940 cases were reported to US law enforcement: online auction fraud accounted for 25.5% of the reported cases and 16.3% of the total loss; payment card fraud accounted for 9% of cases and 4.7% of the total loss; and Nigerian advance fee scam accounted for 2.8% of cases and 5.2% of the total loss. The total monetary loss from all reported cases of internet fraud and scams to United States law enforcement agencies in 2008 was US$264.6 million – an increase of 10% from the 2007 [14].

MALWARE CREATION AND DISSEMINATION

The McAfee 's virtual crime report indicated that cybercriminals are increasingly exploiting vulnerabilities in software and applying social engineering to spawn a broad range of threats including spyware, phishing, adware, rootkits4, and botnets. In 2008, Symantec [20] reported that new malicious code had increased by 265 percent since 2007 and 60 percent of all current malicious code was detected in 2008. Malware5 is software designed to infiltrate, compromise security or damage a computer system, without the owner's informed consent and includes viruses, worms6, backdoors, keyloggers, and trojans. The 2008 UK Threat Assessment report observed that 'most new malware is designed to steal financial data (such as credit card details, bank account details, passwords, and PINs) as a precursor to various frauds and other deceptions' [22]. An example of information stealing malware is keylogging programs that are designed to monitor user activity including keystrokes. This can then be used by cybercriminals to steal passwords or credit card details, which can then be used for malicious purposes such as identity/online fraud. An example of a 'keylogger' case was the attempted theft of more than £229m from Sumitomo Matsui Banking Corporation in London. Three individuals were extradited to the UK from Belgium and Spain and £1.5m in assets was [reportedly] restrained [23]. [7], estimated that the number of potentially malicious threats emerging each month increased from roughly 300 to 2,000 between 2003 and 2005, largely due to the growth of bot-malware. [4], an IT security company, noted that an unpatched computer without antivirus protection or a firewall would have a 50

percent chance of becoming a zombie within 30 minutes of being connected to the internet. Bot malware are often surreptitiously forwarded to victims by various means, such as via email attachments, peer-to-peer (P2P) networks, and visits to an infected website. Building botnets requires minimal levels of expertise [22]. Bot malware typically takes advantage of system vulnerabilities and software bugs or hacker-installed backdoors that allow malicious code to be installed on computers without the owners' consent or knowledge. Compromised computers (also known as bots) are then turned into zombies. The shift in motivation from curiosity and fame seeking to illicit financial gain has been marked by a growing sophistication in the evolution of bot malware, as illustrated by recent examples of detected bot malware such as Conficker. Conficker has received a considerable amount of media attention, and has been reported to have successfully infiltrated government networks, home PCs, critical infrastructure, and universities [7]. According to analysis of the Conficker and its variants (Conficker B and C) by Sophos and the Malware Threat Centre at SRI International, Conficker was designed to provide a secure binary updating service that effectively allows the bot malware designer instant control of millions of PCs. The design included sophisticated defensive mechanisms such as binary encryption methods and compiler-level code obfuscation to hinder detection by anti-malware software. Reverse engineering was made more difficult for investigators analysing the malware (Porras et al. 2009; Fitzgibbon & Wood 2009) Compromised computers – zombies – can then be used as remote attack tools or to form part of a botnet under the control of the botnet controller. According to [3] bot networks accounted approximately 90 percent of all spam email in 2008. A 2008 report by [2] also stated that 'the number of compromised zombie PCs in botnets has quadrupled in the last quarter alone and that these are capable of flooding the Internet with more than 100 billion spam messages per day ... [and] are increasingly switching to phishing, distributed denial of service (DDoS) and website attacks which are capable of causing a huge amount of damage and are a growing threat to the security of nations, the national information infrastructure, and the economy.' [14]. Although malware are still disseminated using conventional tools such as email, cybercriminals have turned recently to exploiting browser plug-in and webserver vulnerabilities. A large number of commercial, government, university and other high profile and high traffic websites worldwide apparently may have been successfully compromised to allow 'infection' of unwitting visitors with malware. For example in May 2009, the UK regional director of Finjan, an IT provider of secure web gateway solutions, noted that a botnet discovered by the company in February 2009 contained 1.9 million infected computers including 73 government domains [11]. Similarly in the first quarter of 2009, [10], reported an increase in the number of malicious websites created and 'sites that host malware—with thousands of new sites appearing daily'. They also discovered a search engine–optimization ring that targeted the top Google search terms to enable the installation of anti-virus software. Business, government and individual householders need to be aware of risk mitigation strategies and implement and update them because search engine optimization will continue

to be one of the most sought after attack vectors by criminals.

RESPONSES AND COUNTER MEASURES

The threat of cybercrime has given rise to a demand for strategies for prevention and control, particularly in the area of OC in cyberspace. Some of the key approaches reduce opportunities for the commission of cybercrime, making such activities more difficult to commit, increasing the risks of detection, enhancing the level and certainty of sanctions, and reducing the benefits likely to be derived from committing such crimes. For example in the context of keeping children safe online, international treaties such as the Council of Europe (CoE) convention on the protection of children against sexual exploitation have been introduced to deal with child sex offences. A recent report, for example, pointed out that countries, particularly common law jurisdictions such as Australia, Canada, Singapore, United States and United Kingdom have introduced online child grooming offences and laws that regulate the behaviour of sexual offenders on release from custody, such as sex offender registration and community notification [13]. Anticipating the likely actions of transnational criminals and terrorists is a key role of law enforcement agencies (LEAs). The effectiveness of these responses is debatable given the hierarchical nature of LEAs, inter-agency rivalry and organisational pathology deemed to exist within some intelligence systems [2]. In our increasingly interconnected world, threats to national security can come from unexpected sources and directions. OC and cybercrime appear to have grown in volume and impact, and both will increasingly affect the financial security of online business in addition to continuing to cause social harm to individuals and social cohesion [6]. The widespread incidence of identity theft, including online theft of virtual identities, for example, is a major challenge since such theft is a common precursor offence that requires a broad-based prevention effort [9]. Furthermore, the potential for mitigation of transnational cybercrime lies in effective public-private partnerships. The role of public policing agencies will be a necessary but only one part of the overall response to cybercrime [13]. Convincing relevant private sector actors of the need to cooperate in crime prevention, and forging regional multi-lateral cooperation between jurisdictions in partnership with the public sector, are key challenges [17]. The 'securitisation' process evokes a crisis-like security context in order to permit extra-ordinary measures to reduce risk. How this may occur in a multi-lateral context, where harmonisation of response to non-traditional security threats is relatively novel, is the immediate challenge for effective control of cybercrime 'anarchy' [23]. Greater knowledge, and the recognition of a sense of 'shared fate' in cyberspace, will quicken the development of multilateral responses and the capability for transnational crime control. OC and terrorist groups have also recognised the value of leveraging information and ICT to facilitate, or enhance the commission of crimes, and are dynamic in identifying new opportunities and ways to overcome counter-measures. Extraterritoriality, the notion that cyberspace has no geographic boundaries has driven the e-commerce revolution, but OC also operates online under the same free market principles. The emergence of an underground economy as the source/provider of illicit

information may now indicate the level of professionalism and commercialisation present in the transnational crime sector. The illicit enterprise nature of the current digital underground market is an example. OC activities in cyberspace have serious implications for national security, and trends in cybercrime have shown that attacks are increasingly originating from regions where sanctions are often non-existent or operate as 'on-costs,' and enforcement is less robust. The need for greater uniformity/harmonisation of cybercrime legislation within Australia and across the region will become more pronounced as the number of cybercrime cases increases as forecast [4]. Existing legislative regimes, despite attempts at definitional 'technical neutrality', remain vulnerable in the context of rapidly emerging, new generation technologies to commit crimes [23]. In addition, existing offence definitions, although technically adequate, may be impossible to apply in practice [3]. For example, in the case of the prosecution of 'botnet' intrusions, evidence would need to be obtained concerning each of the thousands of computers that have been compromised – a gargantuan task. Thus a new offence category, such as creating a network for illegal purposes and selling/renting established botnets (networks of compromised computers) to commit or facilitate criminal activities, could be developed to deal with these threats. The true impact of cybercrime is unknown due to poor detection and under-reporting, but cybercrime prosecutions involving multiple jurisdictions will be an essential response [22]. Because online offending easily transcends borders easily, numerous territories can simultaneously assert jurisdiction, particularly when an attack transits multiple jurisdictions with different regimes for preserving evidence. Timely access to evidence located in one or more foreign jurisdictions may be difficult or impossible, as it would normally require the assistance of authorities in the foreign jurisdiction(s), who may be unwilling or unable to assist. When the suspect is located abroad, these difficulties are compounded. Countering the risks of cybercrime is a multi-dimensional challenge and requires effective coordination and collaborative efforts on the part of a wide range of government and private sector entities. Achieving some uniformity will be an essential strategy to minimise the risk of so-called safe havens and 'jurisdiction shopping', in which offenders seek out countries from which to base their activities that have the least severe punishments or which have currently no extradition treaties. A recent report by the Commission of the European Communities [7], for example, highlighted the need to enhance cross-border law enforcement and judicial cooperation in the fight against transnational payment fraud, and improve the response of the UN, Interpol and other international agencies efforts [9]. The level of mutual legal assistance in the China and ASEAN region is underdeveloped, particularly in respect to cybercrime, while Internet penetration has grown rapidly (Thomas 2009). China, for example, now has the largest population online, exceeding the USA. The CoE's Cybercrime Convention [5] is an apt model legislation that has been adopted by some Asian jurisdictions (e.g. Japan & Philippines) and has been influential in the development of new laws in Thailand and Indonesia [9]. A recent review of the legislative coverage or criminalisation of cybercrime in Asia8 showed that many gaps continue to exist in the 'seamless web' of laws designed to counter cybercrime in the region [10].

Microsoft used the CoE Cybercrime Convention bench-mark, and, noted the poor compliance with model privacy laws and only one jurisdiction met the modest 'opt-out' anti-spam regime benchmark applied. Even for core offences such as the criminalization of unauthorized access to computers, systems, programs and data some countries had yet to enact laws or provide for civil remedy. Despite widespread public alarm only one jurisdiction met the model laws for on-line child safety and six countries were without relevant laws. In short the scope of legal countermeasures to common cybercrime offences provide ample manoeuvre for offenders wishing to exploit cross-border legal loopholes [14].

THEORETICAL PROBLEMS

The absence of settled theory about the interaction of OC with cyberspace is an impediment to the development of sound countermeasures. At present, crime prevention practices based on actor choice (cf. neo-classical deterrence theory) are usually applied with variable effect [14]. Routine activity theory draws on rational exploitation of 'opportunity' in the context of the regularity of human conduct [14], to design prevention strategies, especially where terrestrial interventions are possible – for example in the transit of goods. This approach assumes criminals are rational and appropriately resourced actors that operate in the context of high-value, attractive targets protected by weak guardians (e.g. ill-managed ISPs and jurisdictions with weak legal enforcement of the Internet). An assumption is that OC are profit-focused enterprises that seek out opportunities provided by cyberspace, and acquire the necessary resources for cybercrime by (inter alia) using delinquent IT professionals and targeting weakly protected computers/networks or other digital devices. Consequently, deterrence (increased penalties and detection) is the preferred policy response enhanced by appropriately trained police (capable guardians) and target 'hardening.' The myriad motivations of offenders requires no elaboration in the rational-choice model, and prevention strategies should be as effective against terrorists using the Internet as they would be for individual 'hackers' seeking reputation, or OC seeking illicit gain [12]. However, such an assumption in respect to some forms cybercrime may be misplaced. There is an absence of evidence-based research about offender behaviour and recruitment in cyberspace, although learning and imitation play important roles [22]. Hence, OC groups cannot be understood from just their illicit activities alone, that is – as rational profit-driven networks of criminal actors, since socio-cultural forces play an important role in the genesis and sustainability of such groups. Alternative theoretical approaches that posit particular offender motives or pathologies, or the role of social conflict, have not featured widely in explanations of cybercrime. Early accounts of 'hackers' emphasised individuality and a non-profit orientation, but also observed the likely shift to profit oriented misuse as the Internet developed [7]. Indeed the role of social learning and offender pathology has been neglected but may play a significant role in predisposing some actors to criminal activity and risk-taking in cyberspace, where anonymity reduces social surveillance and self-control [5]. Hate and so-called 'content' crimes perpetrated via the Internet may reflect social or individual pathologies, and less

the exercise of rational choice – although it may be 'rational' to adopt Internet strategies of dissemination [7]. Functionalist approaches assume crime is a normal adaptation to change, and indeed represents a creative response to adversity (usually experienced as different forms of social exclusion) – cybercrime in this sense is normal, although novel in its form. Thus, the cost of suppression of cybercrime may only be achieved by curtailment of the Internet's natural advantages, such as low-cost connectivity. Another approach is to see the rise of certain forms of crime as a result of conflict within society and disputes about what constitutes 'real' crime: here, the criminalisation of an act represents the exercise of power by elites. Thus, defining behaviour as deviant or criminal may represent only sectional interests with little real community support. For example, the practice of illegally copying digital media without paying the copyright holders has only been recently 'criminalised,' with attendant changes to community attitudes, opportunities for criminals and policing practice. [9], noted that in order 'to advance criminological theory we need a developed theory of action through which we can address causal mechanisms.' Functionalist, learning and conflict explanations, as well as choice theories, are often applied to explain OC. In the context of cyberspace, we have limited understanding and empirical sources about these 'causes' with respect to profit and content forms (e.g. hate crime, child pornography etc) of cybercrime. We therefore propose the following: 1. The extent of profit-oriented cybercrime will index OC activity in cyberspace, and the more lucrative, the more likely OC rather than individual offenders will dominate, and – the corollary that – content-related cybercrime will reflect 'pathology' and be dominated by individuals rather than OC. 2. Criminal networks operating in cyberspace will tend to be new forms of OC rather than traditional 'mafia'-like groups. Traditional OC will have limited operations and focus on precursor offences such as identity theft or money laundering. 3. OC operating in cyberspace will trade primarily in the protection of illicit data and information (e.g. compromised credit card and identity details) and less likely to be engaged in systematic fraud/deception-related cybercrimes. These propositions offer challenging research questions and are conditioned by the way we see cybercrime evolving with the advent of technological and behavioural changes among those who use the internet

FUTURE TRENDS

The use of 'bots' is expected to increase in the near future. Botnets are expected to become involved in more sophisticated, targeted attacks and reflects a general trend toward more focused hacker attacks [10]. While 'syntactic' attacks such as worms and viruses were previously spread to cause disruption and inconvenience, the use of 'semantic' or social engineering methods such as 'pharming' 9 are used to steal personal information that may be used to access bank accounts [13]. Therefore OC is expected to adopt this activity and take a more active role in future high tech crime. There will be a shift in targets from desktop computers to smart devices (i.e. cellular phones, Blackberry's) and other such internet-linked personal organizers partly due to the ordinary user's inclination to store confidential information such as bank pins on such

devices. These are expected to become the next prime target for attacks [13,18]. The introduction of commercial appliances linked to the internet (e.g. vending machines, gas pumps, ATM's) and the increased usage of mobile phones to pay for such products suggests that this will be the target of malware in the future. Other non-PC devices will also be targeted. This includes routers, switches and backup devices. Furthermore, real-time programs such as IM (Instant Messaging) are likely to be increasingly targeted in the near future and are rapidly becoming a major risk vector [19]. There appears to be a trend towards a greater emphasis on the development of semantic/human intelligence methods rather than the syntactic measures. This is due to semantic methods placing value on particular types of information (i.e. credit card information) rather than the use of syntactic methods to release viruses and denial-of-service attacks. Human based social engineering is able to obtain information in many cases that technological methods are unable to. This further illustrates the changing trend towards profit-motivated attacks and the involvement of OC [19].

CONCLUSION

A 2007 inquiry into the future impact of serious and organized crime on Australian society raised concerns about '...the increasing use of technology, transnational connections and fluidity of organized crime groups [that] will make law enforcement's task of policing organized crime's illicit activities more difficult' [11]. In the inquiry, the Australian Crime Commission '...called for a greater involvement and contribution by academia to the body of research informing Australia's policy and operational choices in fighting organized crime' [12]. The importance of looking ahead to future offending in the online environment was highlighted by [4] who, only five years ago, noted that crime in the digital environment was prone to rapid change and 'those who fail to anticipate the future are in for a rude shock when it arrives.' There is need for further research. An urgent research project would be to launch region-wide studies of the cybercrime threat environment that aim to address the impact of OC involvement in cybercrime, the nature of new variants of cybercrime and the response of regulators. Such research would need to entail an extensive multi-method approach to data collection designed to address the following questions: 1.What are the current trends and emerging challenges that impact on cyber-security, specifically the use of new and emerging technology to facilitate and/or commit cybercrime? 2. What is the extent of the shift toward OC cybercriminal activities and what are the characteristics of OC online activities? 3. What are the best practices in responses to cybercrime and the best ways regulatory agencies can minimise the risks of cybercrime? 4. What are the challenges for LEAs in detecting and prosecuting cybercriminal activities and what new technologies are needed to combat cybercrime? 5. What prevention strategies best help individuals and corporations avoid cybercrime risks? Such an agenda would help fill gaps in the knowledge base about cybercrime, and provide a vital regional perspective. In addition, the research enhances greater collaboration within the international community that will allow law enforcement agencies, policy makers and other key stakeholders to better understand and manage potential

cybercrime threats in their jurisdictions, regions and globally.

REFERENCES

1. Australian Government Department of Defence. (2009) Defending Australia in the Asia Pacific century: Force 2030. Online. Available
2. HTTP:http://apo.org.au/sites/default/files/defence_white_paper_2009.pdf (accessed 31 July 2009).
3. Brenner, S.W. (2002) 'Organized Cybercrime? How Cyberspace May Affect the Structure of Criminal Relationships', North Carolina Journal of Law & Technology, 4:1, 1-50.
4. Brenner, S.W. &. B.A. Frederiksen, (2002) 'Computer Searches and Seizures: Some Unresolved Issues', Michigan Telecommunications & Technology Law Review, 8:39.
5. Brenner S (2006) 'Cybercrime Jurisdiction', Crime, Law and Social Change, 46: 189-206.
6. Brenner S (2007) '"At Light Speed": Attribution and Response to Cybercrime/Terrorism/Warfare', Journal of Criminal Law and Criminology 97:2 379-475.
7. Broadhurst, R. 2005. International Cooperation in Cyber-crime Research, presented at the 11th UN Congress on Crime Prevention and Criminal Justice, Workshop 6: 'Measures to Combat Computer Related Crime', Bangkok, April, 2005.
8. Broadhurst, R & P. Grabosky (2005) Computer-Related Crime in Asia: Emergent Issues. In Broadhurst, R. & P. Grabosky [Eds.], Cybercrime: The Challenge in Asia, Hong Kong: The University of Hong Kong Press, 347-360.
9. Broadhurst, R G and Chantler, A. (2006) 'Cybercrime Update: Trends and Developments', In: Expert Group Meeting on The Development of Virtual Forum against Cybercrime Report, June 28-30, 2006, Seoul Korea, KICJP & UNODC, pp. 21-56.
10. Center for Strategic and International Studies (CSIS). (2008) Securing 17 Cyberspace for the 44th Presidency. Washington, DC: Center for Strategic and International Studies.
11. Chantler A. (1996) Risks, The Profile of Computer Hackers, PhD Thesis, Curtin University, unpublished.
12. Chantler A.N. & R. Broadhurst. (2008) Social Engineering and Crime Prevention in Cyberspace', paper presented to the Korean Institute of Criminology, October 30, 2008, Seoul.
13. Choo KKR (2007) 'Zombies and Botnets', Trends & Issues in Crime and Criminal Justice, 333. Canberra: Australian Institute of Criminology. Online. Available HTTP:
14. http://www.aic.gov.au/publications/current%20series/tandi/321-340/tandi333.aspx (accessed 31 July 2009).
15. Choo KKR (2008) 'Organized Crime Groups in Cyberspace: A Typology', Trends in Organized Crime 11:3, 270–295.
16. Choo KRR (2009) Online Child Grooming: A Literature Review on the Misuse of Social Networking Sites for Grooming Children for Sexual Offences. Research and public policy series no. 103.

Canberra: Australian Institute of Criminology. Online. Available HTTP:

17. http://www.aic.gov.au/en/publications/current%20series/rpp/101-120/rpp103.aspx (accessed 31 July 2009).
18. Choo KRR, Smith RG & McCusker R. (2007) Future Directions in Technology-Enabled Crime: 2007-09. Research and public policy series no. 78. Canberra: Australian Institute of Criminology. Online. Available HTTP:
19. http://www.aic.gov.au/publications/current%20series/rpp/61-80/rpp78.aspx (accessed 31 July 2009).
20. Choo, KKR and RG Smith. (2008) 'Criminal Exploitation of Online Systems by Organized Crime Groups', Asian Journal of Criminology, 3:1, 37–59.
21. Cooke E, Jahanian F, McPherson D. (2005) 'The Zombie Roundup: Understanding, Detecting, and Disrupting Botnets'. In: SRUTI'05 Workshop Proceedings. USENIX Association, Berkeley CA, pp 35–44.
22. Council of Europe. (2004) 'Summary of the Organized Crime Situation Report: Focus on Cybercrime', Octopus Interface conference: Challenge of Cybercrime, September 15-17,
23. Strasbourg Dandurand Y, Colombo G & Passas N. (2007) 'Measures and Mechanisms to Strengthen International Cooperation among Prosecution Services', Crime, Law and Social Change, 47:4–5, 261–289.
24. Felson, M. (1998) Crime and Everyday Life, New York: Pine Forge Press. Fitzgibbon N & Wood M. (2009) Conficker.C: A Technical Analysis. Online. Available HTTP: 18
25. http://www.sophos.com/sophos/docs/eng/marketing_material/conficker-analysis.pdf (accessed 31 July 2009).