The cyber threat landscape: Challenges and future research directions

Kim-Kwang Raymond Choo*

School of Computer and Information Science, University of South Australia, Mawson Lakes campus (Room F2-28), Mawson Lakes, SA 5095, Australia

ARTICLE INFO

ABSTRACT

Cyber threats are becoming more sophisticated with the blending of once distinct types of attack into more damaging forms. Increased variety and volume of attacks is inevitable given the desire of financially and criminally-motivated actors to obtain personal and confidential information, as highlighted in this paper. We describe how the Routine Activity Theory can be applied to mitigate these risks by reducing the opportunities for cyber crime to occur, making cyber crime more difficult to commit and by increasing the risks of detection and punishment associated with committing cyber crime. Potential research questions are also identified.

1. Introduction

The culturally and economically open nations of Australia, United Kingdom (UK) and the United States (US) have thrived on the wealth that information and communications technologies (ICT) have enabled. However, just as ICT provide new opportunities for governments and businesses to operate and expand their presence and reach, ICT also present opportunities for those with criminal intentions and leaves us, as individuals, communities, organisations and as a nation, highly exposed to the threat of cyber attack and cyber crime. New media channels such as Facebook and Twitter, for example, allow individuals to voice their opinions easily, without the need to go through intermediaries (e.g., printed media) and to play a more active role in shaping the societal and political landscapes online – as we see the events in Egypt and its neighbouring countries unfolding since late 2010. On the other hand, minority views such as extremist and subversive views that might not have been heard in the past are more able to receive exposure. Terrorist groups tend to conduct attacks that are highly visible and which result in mass casualties. The nature of cyberspace makes both of those objectives hard to achieve. However, these new media channels can be used as a medium for propaganda such as publishing doctrines promoting extremism activities, recruitment and training of potential terrorists, and transferring information. For example, Jihad-oriented sites are designed to facilitate radicalisation among the Muslim community, and enable individuals linking up with like-minded people and making contact with extremists from overseas involved in terrorist recruitment and financing using new media channels. These channels target the digital generation (the young and the internet-aware), particularly among the Muslim community. The latter, particularly those with a shallow understanding of

---

* Tel.: +61 8 8302 5876.
  E-mail address: raymond.choo.au@gmail.com.

their religion, could be easily misled by the propaganda posted on these channels Choo (2008).

An open nation cannot shut down its cyber systems for fear of these threats. Instead it must build the national resilience needed to maintain an open yet secure cyberspace. To mitigate cyber criminal risks and make informed decisions about cyber security, it is essential to have a clear understanding of the threat landscape and look ahead to future offending in the online environment. This paper seeks to contribute to a better understanding of this ever-evolving cyber threat landscape by providing a snapshot of several risk areas (mainly focusing on financially-motivated cyber criminal activities). Criminological theories based on choice theories can be applied to explain cyber crime. As an example, we explain how the Routine Activity Theory can help to inform and enhance cyber crime prevention strategies.

2.   The cyber threat landscape: an snapshot

In our increasingly interconnected world, threats to our national (and cyber) security can come from unexpected sources and directions. This is what one may label as a 360-degree challenge. In recent years, cyber exploitation and malicious activity are becoming increasingly sophisticated, targeted, and serious. The Australian Government Defence Signals Directorate, for example, reported that an average of 700 cyber incidents targeting Defence networks were detected in 2010 — an increase of 250% from 2009 (AAP 2010). More recently in 2011, the parliamentary computers of at least 10 Australian Federal ministers, including the Prime Minister, Foreign Minister and Defence Minister, were reportedly compromised (Benson, 2011). The 2010 report to US Congress by the US-China Economic and Security Review Commission also indicated that the number of reported incidents of malicious cyber activity targeting US Department of Defense's system has been on the increase since 2000 — see Table 1.

Cyber crime is not a victimless crime. Examples of short and long-term impacts of cyber crime on their victims include:

Table 1 — Number of reported incidents of malicious cyber activity targeting US Department of Defense's system from 2000 to 2009.		
Calendar year	Number of reported incidents of malicious cyber activity	Percent increase from previous year
2000	1415	N/A
2001	3651	158.02%
2002	4352	19.2%
2003	9919	127.92%
2004	16,110	62.42%
2005	23,031	42.96%
2006	30,215	31.19%
2007	43,880	45.23%
2008	54,640	24.52%
2009	71,661	31.15%

Adapted from US-China Economic and Security Review Commission, 2010: Fig. 1.

Short term impact

- Impacting the daily activities of individual end users (e.g. affecting their ability to receive up-to-date information and carrying out financial transactions such as withdrawing cash from ATMs)
- Impacting the day-to-day activities of businesses and government. This can result in significant financial and other losses to businesses, such as exposure to law suits (e.g. in cases involving breaches of customers' data) and increase in operational costs (e.g. losses due to fraudulent activities and increase in security spending).

Long term impact

- National security breaches (e.g. the incident in 2010 where classified/confidential government information was leaked to Wikileaks).
- Social discontent and unrest (e.g. loss of public confidence in the government even if the actual damage caused by the cyber criminal activities was minimal).
- Loss of intellect property, which can affect the long-term competitiveness of businesses and governments in industrial and military espionage incidents.

The million-dollar question is "**How prevalent is financially-motivated cyber criminal activity such as unauthorised access, online extortion and Distributed Denial of Service (DDoS) attacks?**". Official crime statistics compiled by law enforcement, prosecution and other government agencies, and private sector agencies are unlikely to indicate the entire cyber threat landscape. For example, victims were not aware that their organizations had experienced one or more cyber security incidents, and therefore indicated that they had not experienced any such incidents when asked. In addition, victimized organizations may be reluctant to report breaches due to a range of reasons, such as

- believing the incident was not serious enough to warrant reporting it to law enforcement and other competent agencies,
- believing that there is little chance of a successful prosecution,
- fearing negative publicity and that reporting would result in a competitive disadvantage (Richards, 2009).

Victimized organizations may also deal with the incident internally and decided not to report such incidents to an external party, including law enforcement and government agencies.

Cyber threats are increasingly important and strategically relevant in developed economies such as Australia, UK and US. The 2008 report of the Center for Strategic and International Studies (CSIS) Commission on Cybersecurity for the 44th Presidency, for example, reported: 'We began with one central finding: The United States must treat cybersecurity as one of most important national security challenges it faces' (CSIS, 2008). The concern of cyber crime is not only perceived by computer scientists and ICT professionals, but politicians also understand its potential impact as well (Obama, 2009). In 2009, US President Barack Obama remarked:

This world — cyberspace — is a world that we depend on every single day. It's our hardware and our software, our desktops and laptops and cell phones and Blackberries that have become woven into every aspect of our lives. It's the broadband networks beneath us and the wireless signals around us, the local networks in our schools and hospitals and businesses, and the massive grids that power our nation. It's the classified military and intelligence networks that keep us safe, and the World Wide Web that has made us more interconnected than at any time in human history. So cyberspace is real. And so are the risks that come with it. It's the great irony of our Information Age — the very technologies that empower us to create and to build also empower those who would disrupt and destroy. And this paradox — seen and unseen — is something that we experience every day (Obama, 2009).

In Australia, the *then* Prime Minister Kevin Rudd in his inaugural 2008 National Security Statement to Parliament acknowledged that cyber threats now form one of the country's top tier national security priorities (Rudd, 2008). Cyber crime was also identified as one of the four highest priority/tier one national security risks by UK's National Security Council (HM Government, 2010: 27).

Tier One: The National Security Council considered the following groups of risks to be those of highest priority for UK national security looking ahead, taking account of both likelihood and impact.

- *International terrorism affecting the UK or its interests, including a chemical, biological, radiological or nuclear attack by terrorists; and/or a significant increase in the levels of terrorism relating to Northern Ireland.*
- Hostile attacks upon UK cyber space by other states and large-scale cyber crime.
- *A major accident or natural hazard which requires a national response, such as severe coastal flooding affecting three or more regions of the UK, or an influenza pandemic.*
- An international military crisis between states, drawing in the UK, and its allies as well as other states and non-state actors.

It is evident that cyber threats are seen as one of the top issues in crime and national security today, and an increasingly challenging policy area for governments — **Cyber space is the new front line**.

2.1. Malicious software (malware)

Malware has consistently been ranked as one of the key cyber threats to businesses, governments and individuals. For example, in 2009 the number of new malware signatures was reported to be just under 2.9 million, a 71 percent increase over 2008 (Symantec, 2010), but more than 286 million new malware variants were detected by Symantec in 2010 (Symantec, 2011).

The shift in motivation from curiosity and fame seeking/thrill-seeking to illicit financial gain has been marked by a growing sophistication in the evolution of malware (Choo, 2011). The latter, further exacerbated by an increase in the

availability of easy-to-use toolkits to build malware, is likely to remain a threat to businesses, governments and consumers in the foreseeable future. The Zeus bot malware creator kit, for example, was sold at a nominal cost — between US$400 and US$700 (Symantec, 2010). Detailed instructions on how to use such kits are readily available, too. Anybody including individuals with limited programming and/or hacking skills could use the purchased kit to create sophisticated malware or launch sophisticated attacks beyond their skill level to steal online banking credentials or sensitive information. More concerning is the study by Symantec (2010: 11) which 'observed nearly 90,000 unique variants of the basic Zeus toolkit and it was the second most common new malicious code family observed in the [Asia Pacific/Japan] region' in the 2009 calendar year. The widespread availability of such toolkit lowers the technical bar to commit cyber crime. Consequently, there is a marked increase in the number of amateur cyber criminals who usually make their money from distributing spam or selling stolen credentials and information. This may result in the unintended consequence of an increasingly pronounced division between the sophisticated and the amateur cyber criminals, and the sophisticated cyber criminals moving more underground (migrating from public forums to more exclusive forums with their partners in crime).

Choo (2011) explained that malware can be broadly categorised into (a) generic malware that targets the general population and (b) customised information-stealing malware targeting specific institutions. An example of the former is bot malware designed to exploit particular vulnerabilities on machines of individual end users, businesses and governments. Such malware can, for example, be hosted on web servers by exploiting vulnerabilities of the servers. Any unwitting visitors to website hosted on the compromised servers and whose internet browsers and/or operating system are unpatched may have their machines infected with the bot malware — an activity also known as a "drive-by attack". As observed by IBM X-Force® (2011), the US continues to reign as the top hosting country for malicious links and more than one third of all malware links are reportedly hosted in that nation. Machines infected with bot malware are then turned into "zombies" and can be used as remote attack tools or to form part of a botnet under the control of the botnet controller. Zombies are compromised machines waiting to be activated by their command and control (C&C) servers. The C&C servers are often machines that have been compromised and arranged in a distributed structure to limit traceability. The computational power of botnets can then be leveraged to orchestrate other cyber criminal activities such as DDoS attacks, disseminating spam and other malware, facilitating phishing and click fraud, and hosting illegal data such as child abuse materials (Choo, 2007).

An example of customised information-stealing malware is phishing-based keylogger (program designed to monitor user activity including keystrokes) that target specific organisations. For example, in 2010, there were several incidents in the US involving cyber criminals sending a targeted phishing email, aimed at whoever was in charge of the organisation's IT operations. By tricking the victim(s) into opening a harmful attachment or visiting a malicious website, the

cyber criminals were able to install the Zeus malware, which includes a phishing-based keylogger component, onto the machine. In addition, the malware could propagate through the organisation's network, enabling cyber criminals to gain access to and/or compromise other workstations and servers. Once the keylogger was installed on the victim's machine, the program then "faithfully" did what it was designed to do (i.e., send harvested account numbers, login credentials and personal information to a compromised collection server, to be collected by cyber criminals). Cyber criminals were then able to initiate funds transfers by masquerading as the legitimate user using the harvested login credentials and personal information. Money could be transferred out of the account using the ACH system that banks use to process payments between institutions and/or using traditional wire transfers. Financial losses due to these fraudulent wire transfers averaged US$100,000 to US$200,000 per victim (McGlasson, 2010). A number of law suits are currently before the courts in US (see *Patco Construction Company, Inc. vs People's United Bank D/B/A Ocean*, Case no No. 2:09-cv-503-DBH of 2011).

The use of individuals, often unrelated to the criminal activity that creates the illicit funds, to transfer money to criminals interstate or overseas is a long standing practice of the criminal fraternity and is no exception in the online environment. These individuals, also known as "money mules", are a consequence of the need for cyber criminals to transfer and disguise the origins of their criminal proceeds (AIC, 2008, Choo, 2008). They are an integral part in a number of financially-motivated cyber criminal cases including the example described in the preceding paragraph. In a typical money mule transaction, an individual is recruited through various means including the use of fictitious online companies that appear legitimate and spam email advertisements offering bogus employment opportunities. Unlike victims of most cyber criminal activities, the money mules are "participants" who provide full consent to the use of their bank accounts to receive and send wire transfers to overseas accounts controlled/owned by the cyber criminals, minus a commission payment (usually between 5 and 15 percent). When arrested by law enforcement agencies, money mules typically have their bank accounts suspended. They can also be criminally liable for their involvement in the money mule transactions. For example, a number of alleged members of the money mule organization responsible for repatriating the proceeds of the Zeus malware attack described in the preceding paragraph to overseas accounts were charged with various offences including conspiracy to commit bank fraud, conspiracy to possess false identification documents and money laundering (FBI 2010).

2.1.1. Emerging attack vectors: smart devices

In recent years, an increasing number of banking and financial institutions and businesses are offering mobile banking and payment services. The increasing use of smart devices including smart phones (e.g. iPhone and Blackberry) constitutes another opportunity for cyber attacks − malware designed and spread onto mobile devices to compromise information such as online banking login credentials and account information as well as other data stored on these mobile devices (Choo et al., 2007; Choo, 2011). In addition, cyber criminals can place malicious mobile applications (apps) disguised as legitimate apps to increase their yield, such as the Geinimi malware. For example, researchers have reported finding malware and potentially malicious software at third-party apps stores targeting the Chinese market. Legitimate versions of the applications in the official Android market appear to be safe, they said. Compromised phones call back to a remote computer for instructions on what to do at 5 min intervals. Then they transmit information on the device's location, its hardware ID and SIM card back to the remote computer (SMH 2010).

Smart devices can also be used to launch DDoS attacks against governments and corporate networks. For example to launch a DDoS attack using the Java Script-based variant of the Low Orbit Ion Cannon software, users are only required to open a JavaScript-enabled Internet browser or visit a website that hosts the program and enter the URL or IP address of a target into the program (see Pras et al., 2011 for an overview of the software). Although this particular tool is not known to be optimized to run on smart devices, such programs have the potential to be used by malicious actors (including individuals with rudimentary computer knowledge) to participate in DDoS attacks from smart devices.

In 2010, Kaspersky Lab reportedly identified more than 1550 mobile malware signatures (Gross, 2010). Symantec (2011: 6) reported a similar observation − 'there was a sharp rise in the number of reported new mobile operating system vulnerabilities − up to 163 [in 2010] from 115 in 2009'. Lookout (2011: 3) also reported that '[a]n estimated half million to one million people were affected by Android malware in the first half of 2011; Android apps infected with malware went from 80 apps in January to over 400 apps cumulative in June 2011'.

Mobile malware while emerging are quite real. Anti-virus and anti-malware applications for mobile devices are still in their infancy despite the emergence of mobile malware. Existing security applications for desktop computers and laptops are generally unsuitable for resource-limited mobile devices, especially 'once the rate of new or mutated malware instances reaches a threshold beyond which it is not reasonable to push [signature] updates' explained Jakobsson and Juels (2009: 11). Industry observers are paying more attention to mobile malware with major security companies starting to offer anti-virus and anti-malware applications for mobile devices (e.g., McAfee® VirusScan® Mobile and Norton Smartphone Security for Symbian, Windows Mobile).

2.1.2. Emerging attack vectors: ATMS and point-of sales (POS) machines

Security researchers and banking and financial institutions have reportedly identified malware designed to record magnetic stripe information and PIN in recent years (Kirk, 2009). For example, several members of an organized crime group were arrested by Russia's Ministry of the Interior for allegedly contracting a malware author through an underground forum to create malware capable of infecting ATMs (Leyden, 2010). Such crimes are often perceived to be more lucrative with less risk compared to other ATM-related crimes such as ATM skimming.

At present, attacks involving the installation of malware are likely to require physical access to the ATM or a port in

which the malware could be uploaded (Kirk, 2009) as these machines are typically not connected to the internet. This would suggest the need to involve insiders or individuals with physical access to the machines. Many vendors own and operate their own ATM or POS terminals. These terminals should be treated as securely as cash registers, as fraudulently tampered terminals can lead to significant financial losses. For example, customer card information and Personal Identification Numbers (PINs) stolen from malware or skimming devices installed at these terminals can be used to create counterfeit cards by organized crime groups. The counterfeit cards can then be sold to tourists for their use while abroad and/or used to purchase goods and withdraw cash from ATMs around the world.

Choo (2011) pointed out that at present, non-bank owners of ATM and or POS terminals typically are not liable for compensating customers who suffer loss as a result of ATM or POS fraud. Hence, there may be little incentive for these non-bank owners of ATM and or POS terminals to develop and install anti-fraud measures at their terminals. Banks and financial institutions, however, continue to deploy security measures as part of their customer service approach. For example, bank customers are typically assured they are not liable for unauthorised transactions on their accounts if they become victims of proven skimming crimes (ACC 2010). Consideration could be given to requiring non-bank owners of ATMs and EFTPOS machines to ensure that the latest security measures are used on their terminals, such as ensuring the points/ports at which the ATM and POS terminals connect to the network are accessed by authorised personnel on a need-to-access basis and not easily accessible to the general public (Choo, 2011).

The increasing involvement of organized crime groups in cyber crime now emphasises the importance of large-scale profit-driven incentives. Based on past successes of cyber criminals and organized crime groups and the relatively low risk and the high return, it is very likely that these malicious actors will continue to develop innovative ways to use the internet to target this particular market and exploit vulnerabilities for fraudulent schemes.

2.2. Culture/environment of insecurity

Commercial off-the-shelf (COTS) products form the backbone of many of our existing systems and networks. It is always cheaper and easier to launch cyber attacks than to defend against them as COTS products notoriously contain security vulnerabilities. It is reasonable to expect no individual ICT end user, business or government agency will be able to patch every single one of them. For example, IBM's trend and risk report from 2010 indicated that '2010 had the largest number of vulnerability disclosures in history − 8562. This is a 27 percent increase over 2009' (IBM X-Force® 2011: 8). However, an attacker only has to find one or more vulnerabilities and exploit the vulnerability or vulnerabilities successfully in order to gain access to the system.

Malware created by financially-motivated cybercriminals to exploit the vulnerabilities in COTS products can also be used against information systems in nation's critical infrastructure. The example highlighted in the 2009 report to US Congress by the US-China Economic and Security Review

Commission suggested that cyber threat is real and the consequences are significant.

In this instance, a first team of hackers, dubbed the "breach team," reconnoitered the firm's network for months. During this phase of the operation, the hackers gained critical information about computer accounts, employee names and passwords, and general network architecture. They mapped network directories to gain intimate knowledge of the contents of the compromised systems. The breach team then identified and exploited network vulnerabilities.

A second team of hackers, dubbed the "collection team," then used information gathered by the first team to collect sensitive information from the firm's network. Though linked to the first team through common attack vectors, the second team used different tools in unique ways, indicating distinct operators. The collection team quickly and efficiently navigated to precise directories and copied specific high-value files, often ignoring other similarly named and co-located files. This approach, given that the team opened none of the targeted files during the collection process, indicated precise knowledge of file contents as a result of the breach team's efforts and very specific tasking.

The collection team then copied the files and transferred them to high-speed "staging servers" within the firm's network. This decreased the attackers' operational footprint on machines known to the firm to contain high-value data, and it centralized activity on machines with high volumes of traffic, where the malicious activity would be more effectively disguised. The team then compressed and encrypted the files and assigned them innocuous names before exfiltrating the data from the firm's network.

The attackers demonstrated impressive professionalism and tradecraft. They discerned and attempted to secure only the most critical files. Throughout the process, the attackers consolidated attacks to one specific region—in the same time zone — in order to conduct activity after work hours in order better to avoid detection. The attackers set up redundant exfiltration channels so as to maximize the volume of data that they could simultaneously steal and to safeguard against errors and failures in the transfer process. Together, the teams accessed the firm's network on more than 150 occasions using dozens of legitimate but compromised account (US-China Economic and Security Review Commission, 2009: 179).

Similar concerns were echoed in McAfee's Virtual Criminology Report 2009 where more than 20 international experts were interviewed 'to assess their opinions on the definition of cyber war, its impact on the private sector and the priority of issues for public discussion' (McAfee, 2009: 2). The report found that '[t]here have been increased reports of cyber attacks and network infiltrations that appear to be linked to nation-states and political goals … while we have not yet seen a "hot" cyber war between major powers, the efforts of nation-states to build increasingly sophisticated cyber attack capabilities, and in some cases demonstrate a willingness to use them, suggests that a "Cyber Cold War" may have already begun' (McAfee, 2009: 2). Several highly-publicised incidents including the DDoS attacks targeting websites belonging to the U.S. government and intelligence agencies, South Korean government agencies, and Estonia government agencies were cited in the report.

Another highly-publicised incident includes the incident involving the attack on Google® and several other companies in China at the end of 2009. This particular incident included attempts to access the email accounts of certain individuals and steal sensitive information and data (Drummond, 2010). This incident demonstrates how exploits and zero-day exploits in COTS products can be exploited by cyber criminals, state-sponsored or otherwise, to launch sophisticated attacks against individuals and businesses. A more recent high profile example is "Stuxnet" — a malware targeting supervisory control and data acquisition (SCADA) systems used to manage large-scale industrial control systems (ICS) at industrial facilities. Analysis of Stuxnet suggested that the malware was designed to reprogram the ICS 'by modifying code on programmable logic controllers (PLCs) to make them work in a manner the attacker intended and to hide those changes from the operator of the equipment' and the malware consists of '[several] zero-day exploits, a Windows rootkit, the first ever PLC rootkit, anti-virus evasion techniques, complex process injection and hooking code, network infection routines, peer-to-peer updates, and a command and control interface' (Falliere et al., 2010: 1—2). The malware was widely believed to have been designed to sabotage Iran's nuclear power plant centrifuges (Markoff, 2010).

When a government or large commercial network comes under cyber attack, it is not immediately apparent whether the source of the attack is a skilful teenager, an organised cyber-crime group (including politically- and issue-motivated groups), or a nation state. In fact, it may involve two or more of these (Choo & Grabosky forthcoming). Accurate attribution of cyber attacks is no straight-forward task, and moreover questions such as "**How can we determine whether an attack is criminal or an act of cyber war?**" remain. Making a distinction will enable us to identify the appropriate response to each of the threats, such as who is best placed to do what, and determine the rules of engagement. Unfortunately, it has not been an easy task trying to distinguish between the two in all cases or to find the smoking gun to point to. In addition, governments may not use civil servants to perform their "dirty work". They can turn a blind eye to cyber criminal activities that are seen as serving state interests, or offer active encouragement to cyber criminals (Choo & Grabosky, forthcoming). For example, a particular government may tolerate cyber criminal activities to a certain extent as long as the attack is targeted towards foreign interests and fit their political agenda, but once the attacks are against their own interest, they are likely to clamp down on such activities.

The sophistication, scale and the persistent nature of these recent high profile incidents (e.g. incidents involving the Estonia government agencies, Google® and several other companies in China and Stuxnet) have written a new chapter in the history of cyber security. Their effects could, potentially, continue to resonate for months or years to come. Successful attacks on SCADA systems could have undesirable and catastrophic consequences. These include equipment being forced to operate beyond its intended design and safety limits, resulting in cascading system malfunctions and shutdowns such as the collapse of an entire electricity grid; or operating procedures or conditions being manipulated to slow the effort of restoring essential services. It is evident that cyber attacks are getting more sophisticated and going under the radar and most victims only realize they are under attack when it is either too late or months later, when data and corporate secrets have been stolen by the intruders.

2.3. Phishing attacks

Choo, Smith and McCusker (2007) explained that cyber attacks can either be a so-called "syntactic" or "semantic" attack, or a combination of these — so-called "blended" attacks. A syntactic attack is one that exploits technical vulnerabilities in software and hardware to commit cyber crime. Examples include installation of malware on systems to steal data as described in Section 2.1. Semantic attacks, on the other hand, exploit social vulnerabilities to gain personal information. Examples include scam solicitations and online auction fraud. In recent years, there is a continuing movement from either of the above attacks to blended attacks — that is attacks using technical tools to facilitate social engineering in order to gain privileged information. Blended attacks include phishing attacks (social engineering) facilitated by publicly available personal information from new media channels such as social networking sites (Choo et al., 2007). For example, the study released by McAfee in August 2011 found that in a five-year targeted attack involving 72 identified compromised parties by one specific actor — named "Operation Shady RAT" (Remote Access Tool) by the McAfee team,

> [t]he compromises themselves were standard procedure for these types of targeted intrusions: a spear-phishing email containing an exploit is sent to an individual with the right level of access at the company, and the exploit when opened on an unpatched system will trigger a download of the implant malware. That malware will execute and initiate a backdoor communication channel to the Command & Control web server and interpret the instructions encoded in the hidden comments embedded in the webpage code. This will be quickly followed by live intruders jumping on to the infected machine and proceeding to quickly escalate privileges and move laterally within the organization to establish new persistent footholds via additional compromised machines running implant malware, as well as targeting for quick exfiltration the key data they came for (Alperovitch, 2011: 3).

Phishing is generally defined as online scams that frequently use unsolicited messages purporting to originate from legitimate organisations, particularly banking and finance services, to deceive victims into disclosing their financial and/or Personal Identity Information (PII) to commit or facilitate other crimes (e.g. fraud, identity theft and theft of sensitive information). In August 2010, for example, RSA Anti-Fraud Command Centre reported a total of 17,935 phishing attacks — a seven percent increase from the previous month, and the 'bulk of the increase resulted from attacks targeted at a handful of financial institutions which is typical of phishers who prefer to focus their effort on a targeted group rather than spread their attacks across the board' (RSA 2010: 3). Various other studies often singled out the banking and finance services industry as one of the most targeted industry sector in phishing attacks in recent years. For example, the study by IBM X-Force® (2011) reported that financial institutions were

the dominant target of phishing emails in both calendar years 2009 and 2010, accounting for 60 percent and 50.1 percent of phishing targets respectively.

Phishing is not a victimless crime. Ponemon Institute (2011) reported that phishing is one of the top five most expensive cyber crime in both financial years 2010 and 2011 (i.e. 1 July 2009 to 30 June 2010, and 1 July 2010 to 31 July 2011 respectively). Phishing is often associated with other criminal activities such as identity theft, credit card and bank fraud and other financially-motivated cyber criminal activities. Victims include both individuals and organizational entities in the public and private sector. Although the banking and finance services industry is often the target for phishing attacks (and other cyber criminal activities) and suffers a loss as a result, the actual victim is typically the customer who receive the phishing messages and are the subject of the "intrusion", explained Choo (2011). Other potential victims include high-value targets such as top executives/high net worth individuals and employees with financial delegation with the aim of gaining access to corporate online banking systems. For example in January 2009, the

> *vice president of manufacturing [at Experi-Metal reportedly] received a phishing e-mail telling him to fill out what appeared to be a mundane piece of online paperwork: a "Comerica Business Connect Customer Form." He forwarded the e-mail to Controller Keith Maslowski, who then logged into a website belonging to the criminals. With Maslowski's login credentials, the criminals were off and running. Over the next six-and-a-half hours they raced to steal as much of Experi-Metal's money as they could before their window of opportunity closed* (McMillan, 2011a).

Cyber criminals are always on the lookout for new attack vectors for phishing including smart devices (as explained in Section 2.1.1). In addition, such devices are increasingly being used to store and access sensitive accounts and services, making them attractive to financially-motivated cyber criminals. The following is an example of a blended attack targeting mobile users (AVG 2011).

1. The attack involved a phishing attack, disguised as originating from China Mobile (a major mobile phone operator in China), trying to lure users to believe that this is coming from the website of China Mobile (中国移动通信集团公司) — http://www.10086.cn/.
2. Users clicking on the link will be directed to a phishing site — http://www.1oo86.cn/ (using the letter "O" instead of the digit zero). A mobile application was downloaded and installed on the unwitting user's mobile device. AVG (2011: 19) explained that 'the user would not suspect anything because they expect that an update will be downloaded and installed. The attacker gets another advantage here — if the user sees nothing on their device, they forget about it and leave the malware untouched'.
3. There were two variants of malware, one targeting Android operating system and the other Symbian operating system. When the malware is installed on the device, it performs the following activities:
   a. Downloads a configuration file.
   b. Sends out device information such as IMEI number, phone model, and SDK version.
   c. Writes to a log file.
   d. Allows remote control/monitor the device.

AVG (2011: 20) explained that '[t]he crown jewels of this piece of malware are the "premium SMS charges". The malware is sending text messages to premium rate numbers. Premium Messaging is where a user is subscribed to receive content and is billed by a third party. The charges can be one-time or recurring. The subscribing processed is being monitored by the cyber criminals. The user is being charged premium prices, and their phone bill is increasing. The malware can hide these activities from the user by not listing the send/received text messages'.

In recent times, law enforcement agencies and the judiciary appear to be taking cyber crime including phishing more seriously. For example in July 2011, an individual was reportedly 'sentenced to more than twelve years in federal prison for his center role in an international phishing and email spamming ring that stole the identities of more than 38,000 people' (McMillan, 2011b).

3. Cyber crime prevention strategies: applying criminological theories

Various crime prevention practices are generally based on actor choice (cf. neo-classical deterrence theory). The Routine Activity Theory (RAT), for example, proposes that crime occurs when a suitable target is in the presence of a motivated offender and is without a capable guardian (Cohen and Felson, 1979) — see Fig. 1.

The theory draws on rational exploitation of 'opportunity' in the context of the regularity of human conduct to design prevention strategies, especially where terrestrial interventions are possible — for example in the transit of goods. It assumes criminals are rational and appropriately resourced actors that operate in the context of high-value, attractive targets protected by weak guardians (Felson, 1998; Yar, 2005). In the context of cyber crime, an assumption is that cyber criminals are (1) criminally and/or financially-motivated that seek out (2) opportunities provided by cyberspace such as

Fig. 1 — **Application of Routine Activity Theory in crime.**

anonymity and no geographical limitations, acquire the necessary resources for cyber crime by (inter alia) using delinquent/rogue IT professionals and (3) targeting weakly protected systems/networks and exploiting situations where law enforcement agencies are being hampered by jurisdictional, legislative and evidentiary issues, particularly in cross-border cyber criminal cases (Broadhurst and Choo, 2011).

There are a number of ways that criminological theories such as RAT can be applied to reduce the risk of cyber crime. Cyber crime prevention strategies using RAT, for example, target each of these areas − (1) increasing the effort required to offend; (2) increasing the risk of getting caught; and (3) reducing the rewards of offending − see Table 2.

3.1. Fostering a culture of security

Incubating and creating the market incentives for ICT service or content providers to integrate security into their software, hardware and system development life cycle will lead to an improved level and type of security, and increase the marginal cost of security violations. Consequently, the effort required to offend is increased and the marginal benefits of cyber crime reduced. Secure software and hardware will also result in productivity gains for ICT service or content providers as less time and resources will be spent on formulating and releasing patches (Choo, 2010).

Organizations actively seeking to go beyond mere compliance with existing legislation will generate consumers' trust and confidence and thus, result in competitive advantage in the new world of informed consumers. However, higher levels of security can only be achieved at higher marginal costs. One possible solution is to create an environment conducive for ICT service or content providers to achieve marketing and competitive advantages if they offer products and services with higher levels and more innovative types of security to assist in combating cyber exploitation (e.g., government tenders), as suggested by Choo (2010). Government agencies could also play a major supporting role in assisting software and hardware vendors in developing secure software and hardware components, such as the example involving US's National Security Agency helping Microsoft to develop their Vista operating system to ensure it met the requirements of the Department of Defense (McMillan, 2007).

3.2. Public private partnership (PPP)

No single entity "owns" the issue of cyber security. While governments cannot completely delegate the role of securing cyberspace, governments cannot work in isolation and

a majority of the critical infrastructures sectors − perhaps, with the exception of communist nations such as China − are privately owned. There will never be enough policing resources to investigate all cyber criminal activities, and the role of public policing agencies is only one, albeit important, part of the overall response to cyber crime (Choo, 2011). Vulnerabilities in a particular (online) environment could potentially be exploited by criminals and actors with malicious intent. Tight couplings between industry sectors, particularly between ICT and other sectors, may potentially result in rapid escalation of seemingly modest disruptions within one sector. If any of our unsecured sectors are successfully compromised, these compromised sectors can then be used as launching pads to attack other sectors and disrupt other industry sectors − also known as exploitation of infrastructure (Choo et al., 2007).

Different players in the digital economy are best placed to play different but complementing roles in mitigating the cyber crime risks to consumers, businesses and governments. The potential for mitigating cyber criminal activities, particularly financially-motivated cyber criminal activities, lies in an effective partnership between the public and private sectors. The Commission of the European Communities, 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 (Dandurand et al., 2007).

There is a need for secure and trusted information-sharing mechanisms between the public and private sectors so that timely and actionable cyber alerts, classified or sensitive information can be shared both domestically and across international borders. For example law enforcement agencies can help in developing and validating effective measures and mitigation controls in collaboration with the private sector by sharing classified or sensitive information such as intelligence and software/hardware vulnerabilities discovered in the course of a law enforcement investigation with the manufacturers and vendors. This would enable all parties involved to develop real-time mechanisms for collaborating to stop cyber attacks in progress and investigate cross-border cyber crime. Effective PPP would also ensure that developments in ICT are well understood by policy makers, which was also a recommendation of the Australian Government House of Representatives Standing Committee on Communications (2010) in its report on cyber crime (Recommendation 7) − see Table 3.

3.2.1. Volunteer cyber defenders
In today's ever-evolving cyber threat landscape where cyber attackers are constantly searching for new ways to circumvent

Table 2 − Cyber crime prevention strategies using Routine Activity Theory.			
Cyber crime prevention strategies (Section)	Target areas		
	Increasing the effort required to offend	Increasing the risk of getting caught	Reducing the rewards of offending
Fostering a culture of security (3.1)	Yes	No	Yes
Public Private Partnership (3.2)	Yes	Yes	No
Policing and preventative strategy (3.3)	No	Yes	Yes

Table 3 – Recommendation 7of the 2010 Australian Government House of Representatives Standing Committee on Communications' report on cyber crime.

That the Australian Government consult with major IT security vendors, academia and key industry stakeholders to develop:

- options for establishing a coordinated public-private capacity to provide real-time operational information on a wider range of cyber crime types that impact on Australian consumers;
- an 'intelligence hub' that facilitates information sharing within and across industry sectors and provides:
  - longer term analysis on cyber crime methodologies across a range of cyber crime types;
  - education on the preservation of digital evidence; and
  - support to law enforcement agencies for targeted prosecutions in Australia and overseas.

Australian Government House of Representatives Standing Committee on Communications (2010).

existing security and legislative controls to commit cyber criminal activities, it is essential for cyber defenders to possess up-to-date knowledge, skills, and experiences. It is unrealistic to expect that government agencies have all the cyber security expertise required in securing the nation's critical infrastructures. Furthermore, uncompetitive government salaries and lack of a career path for cyber security professionals can result in a continual brain drain to the private sector. Conti and Easterly (2010: 2), for example, explained that

[US] faces a severe shortage of information security savvy talent. The pool of candidates dwindles even more when considering such constraints as the ability to receive a Top Secret clearance, possession of U.S. citizenship, desire to undergo repeated drug tests, and, in some circumstances, ability to pass a polygraph exam.

The private sector can play an important role in strengthening the nation's cyber security capability. For example, cyber security experts in the private sector can be enlisted to help law enforcement and other government agencies in incident response activities (e.g., conduct forensic examinations and help to attribute source of attacks) and during times of emergencies. One could look to the recently established Cyber Defense League, an Estonian volunteer organization that in wartime would function under a unified military command (Gjelten, 2011), and the Professional Cyber Defender Programme in Singapore (Ho, 2010) as examples of private sector participation in national and cyber security activities. For the private sector, partnerships may result in commercial opportunities and, perhaps, more effective, policing avenues for their clients. In addition, volunteer cyber defenders could participate in cyber security awareness and educational initiatives targeting the general public as discussed in the next section.

3.2.2. Joint user awareness and education initiatives

It is inevitable that we will see an increase in the variety and volume of financially- and politically-motivated cyber criminal activities targeting individual end users, government agencies and businesses. As individual ICT end users, we need to be even more vigilant online and if we do not undertake measures to protect ourselves online, we would be easy targets to the less sophisticated cybercriminals – the lowest hanging fruit. User awareness and education are critical in mitigating cyber threats such as targeted phishing and would enable individuals and business, particularly small and micro businesses, to maintain current knowledge of the latest cyber crime activities and the best cyber crime prevention measures available (Choo, 2011). Messages should be tailored accordingly to target different audiences (e.g. Generation X, Generation Y, and baby boomers; and end users from diverse cultural and linguistic backgrounds) and crime types (e.g. financially-motivated cyber crime and ideologically-motivated crime such as internet-driven radicalisation). Effective education and awareness-raising initiatives can potentially reduce the numbers of unprotected computers that are available for cyber exploitation (e.g. to be used as part of a botnet to launch other cyber attacks).

Although all of us need to take responsibility for protecting ourselves in the online space, a key message from the Australian Government House of Representatives Standing Committee on Communications (2010)'s inquiry was that a more integrated, coordinated and concerted effort by government agencies, industry and community organisations is required to combat the cyber criminal activities that victimize individual end users and businesses, and can help to ensure the most effective cyber crime prevention advice is provided to the community (e.g. campaigns to ensure that individual consumers and front-line police officers know where and how to obtain information on how to protect themselves in cyberspace). An improved understanding of the cyber crime risk environment will also place the society in a much better position to manage new and emerging cyber threats (Choo, 2011).

Longer-term measures should include funding for cyber security education and research, and educating and encouraging individual consumers (and businesses) to report incidents to law enforcement and other competent agencies so that the government has a better understanding of the current and emerging cyber threats and are able to develop responses to neutralise cyber crime opportunities before they arise. Examples include the Action Fraud website where individual consumers and businesses can report fraud and scams to UK's National Fraud Authority 24/7 (See http://www.actionfraud. org.uk/) and US's Internet Crime Complaint Center (See http://www.ic3.gov/default.aspx).

3.3. Policing and preventative strategy

Law enforcement typically operates at three broad levels: crime prevention, investigation and prosecution. As cyber attacks and resultant cyber crime often transcend national frontiers, law enforcement investigations can be hindered by the global distribution and increasingly corporate ownership of ICT infrastructure and services. Consequently, there is a need for law enforcement agencies to reassess policing roles and techniques in order to better attune the delivery of modern day policing to the needs, wants and expectations of the society. In today's increasingly digitalised environment, 'policing will [most likely] be carried out over a borderless community, rather than within the confines of national

boundaries' (Sim, 2000: 116). In traditional criminal cases, for example, international cooperation typically occurs at the end of the law enforcement and judicial process where charges have been formally laid and the accused persons are ready for extradition. However, for cyber crime cases, international cooperation is usually required at the beginning of the investigation process. This can, however, pose a challenge for traditional criminal law and as explained by Brenner and Schwerha,

> [l]aw is at base territorial; criminal laws are promulgated and enforced by nation-states, which use them to control crime and maintain the baseline of internal order that a society requires to survive. Criminal law therefore has been purely domestic; external threats to order that came from nation-states were dealt with by the military, not by law enforcement. (Brenner and Schwerha, 2008: 19).

Although there have been several other high profile success stories involving cross-jurisdictional cyber crime investigations and information sharing, '[t]his has been achieved at practitioner level, rather than as a result of multilateral agreements or cooperation between nations at government level' (Baines, 2008: 1). Using a hypothetical example, an article by the FBI attempted to explain the importance of multilateral cooperation and cyber crime legislation.

> A cyber crook hacks into a bank in Mexico City. Mexican investigators trace the computer used in the attack to New York City, and quickly contact FBI agents, who discover that the New York computer is linked to a computer South Korea. They alert Korean agents, who learn that the attack originated in Bangkok. Thai agents make the arrest. Thanks to the network, the investigative process may take hours or days instead of weeks or months. This level of timely cooperation is essential. But cooperation needs to go hand in hand with consistent laws for cyber crimes, said Christopher Painter, Deputy Assistant Director of our Cyber Division. Uniform penalties must be adopted, or savvy cyber crooks will simply base their operations in countries with the most lax cyber laws. "The bottom line is to make sure there are consequences for criminal cyber actions (FBI 2009: np).

Disparities within and between countries will continue to create risks, and there is a continuing need to enhance cross-jurisdictional law enforcement and judicial cooperation in the fight against cyber crime (Choo et al., 2007). Rita M Glavin — Acting Assistant Attorney General of the United States Department of Justice — also pointed out in her testimony before the House of Representatives Homeland Security Committee Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology in 2011 that

> As illustrated by the array of cases I have mentioned, carders operating in carding forums on the Internet reside in different countries, collaborate freely across borders, and can immediately and widely distribute stolen identity information around the globe. In addition, online carding forums provide networking opportunities for criminals interested in joining together to perpetrate other financial fraud or criminal activity on a global

scale. As a result, coordination and cooperation from foreign law enforcement is vital to the success of carding investigations and prosecutions. In this regard, the Identity Theft Task Force's Strategic Plan also recommended that the Department of Justice and other departments and agencies take specific steps to improve coordination and evidence sharing with foreign law enforcement agencies (Glavin, 2009).

The primary objective of a legislative and prosecution strategy is deterrence. Achieving some measure of uniformity, one possible policing and preventative strategy, will help to is create an environment which is hostile to cyber crime, and minimise the risk of so-called 'jurisdiction shopping' in which offenders seek out countries from which to base their activities that have the least severe punishments or which have no extradition treaties current (Choo et al., 2007).

4.   Conclusion

While cyber criminal and security risks may be seen by some as an extension of existing threats to cyber and national security, the threat landscape is an extremely fast-moving environment. Only seven years ago, several criminologists warned that 'those who fail to anticipate the future are in for a rude shock when it arrives' (Smith et al., 2004: 156). It is essential for our society to be prepared and for our businesses, governments and research institutions to innovate faster than criminals and other actors with malicious intents.

4.1.   The way forward: technical research

To ensure that we continue to have the required capabilities to (1) reduce both the likelihood and consequence of threat against our nation, (2) provide societal security and resilience, and (3) enhance and support digital productivity across society, we need to invest in research and development (R&D) initiatives. Although governments should continue to invest significantly in science, technology, engineering, and mathematics (STEM) education and R&D, there is a need for the private sector to invest in joint R&D initiatives to enable cyber security researchers to play a more significant role in designing state of the art security software and hardware that can be deployed in an online environment. The challenge for the public and private sectors is to design technologies that are robust in the sense that their legitimate use is minimally constrained, but their illegitimate use prevented or discouraged (Grabosky, 2007).

In 2010, Singapore's Senior Minister of State for Law & Home Affairs explained that 'with the ever-changing cyber landscape, we can expect to see adversaries evolve and come up with new threats to circumvent our security defences … [and flagged that it] is therefore necessary for the IT security industry as a whole to step up to the plate to meet this challenge with innovative and strategic solutions against these emerging threats' (Ho, 2010: np). For example,

- How do we address the technical and operational challenges associated with securing fundamental ICT infrastructure against cyber attack and resultant cyber crime?

- How do we more accurately identify, analyse and attribute the source of a cyber attack/incident in a timely fashion?

Fortunately, there are enormous incentives for the private sector to contribute to cyberspace security. A 2010 report, for example, predicted that US 'federal investment in information security will rise from $8.6 billion in 2010 to $13.3 billion by 2015 at a compound annual growth rate of 9.1 percent, nearly twice the rate of overall federal IT spending' (Goldman, 2010).

4.2. An evidence-based policy response

Cyber security research is of a cross-disciplinary nature, and will potentially involve researchers from non-technical domains such as criminology, law, engineering and psychology. There is an ongoing need to conduct more strategic research and evaluation that can provide policy and practice relevant evidence that would enable policy makers and practitioners to design national regulatory measures and appropriate policy responses to address this new emerging cyber threat environment. In mid 2009, for example, the Australian Government House of Representatives Standing Committee on Communications conducted an inquiry into the incidence and impact of cyber crime on consumers and the Australian economy. The committee also examined the adequacy of Australia's measures to combat the problem. There were 34 recommendations outlined in the report tabled by the committee, which can be broadly categorised into (1) regulation; (2) education and research; and (3) public-private partnership (Australian Government House of Representatives Standing Committee on Communications, 2010). The first two recommendations from the Australian Government House of Representatives Standing Committee on Communications (2010) Inquiry into Cyber Crime, for example, stressed the need for greater involvement and contribution of appropriately qualified agencies to lead research that would inform the Australia Government's policy and operational responses to cyber crime.

Potential research projects that would help fill gaps in the knowledge base about cyber crime, and provide a vital regional perspective include:

- What is the nature of cyber crime risks facing the country and its citizens?
- How have cyber crime risks changed in the past few years?
- What are the current trends and emerging challenges that have an impact on cyber crime?
- Has there been any shift from cyber criminal activities perpetrated by individuals to activities perpetrated by organized crime groups?
- What is the financial and other impact of cyber crime on government agencies, business and individuals?
- How much money is lost to cyber crime by government, business and individual end users in the country and region?
- What data sharing mechanisms currently exist between government agencies, and between the public and private sectors for the collection and use of cyber crime data?
- What data sharing mechanisms should be used for cyber crime offences in the country and region?

- What sharing and protection of information processes should be used to facilitate cyber crime research?
- What prevention strategies best help individuals, businesses and government agencies avoid cyber crime risks?
- What international best practice responses exist to dealing with cyber crime, and how can these be used to minimise risks for the nation?

Acknowledgements

REFERENCES

Alperovitch D. Revealed: operation shady RAT. Santa Clara, CA, USA: McAfee Inc; 2011.

Australian Associated Press (AAP). Military faces huge cyber espionage threat. News.com.au 9 October, http://www.news.com.au/technology/military-faces-huge-cyber-espionage-threat/story-e6frfrnr-1225936268254; 2010 [Date last accessed: 06.07.11.].

Australian Crime Commission (ACC). Banks, law enforcement and retailers warn merchants to secure EFTPOS terminals to prevent skimming. Media release 13 April, http://www.crimecommission.gov.au/media/acc_joint/2010/100413.htm; 2010 [Date last accessed: 06.07.11.].

Australian Government House of Representatives Standing Committee on Communications. Hackers, fraudsters and botnets: tackling the problem of cyber crime. Canberra: Commonwealth of Australia; 2010.

Australian Institute of Criminology (AIC). Money mules, High Tech Crime Brief No 16, 2008. Available on: http://www.aic.gov.au/publications/current%20series/htcb/1-20/htcb016.aspx [Date accessed 01.08.2011.].

AVG. AVG Community powered threat report: Q2, 2011, http://www.avg.com.au/files/media/avg_threat_report_2011-q2.pdf; 2011 [Date last accessed: 06.07.11.].

Baines V. Online child sexual abuse: the law enforcement response. In: Doek Jaap, editor. Proceedings of the World Congress III against Sexual Exploitation of Children and Adolescents, Rio de Janeiro, Brazil, 25−28 November 2008, http://www.ecpat.net/WorldCongressIII/PDF/Publications/ICT_Law/Thematic_Paper_ICTLAW_ENG.pdf; 2008 [Date last accessed: 06.07.11.].

Benson S. China spies suspected of hacking Julia Gillard's emails. News.com.au 29 March, http://www.news.com.au/technology/federal-ministers-emails-suspected-of-being-hacked/story-e6frfrnr-1226029713668; 2011 [Date last accessed: 06.07.11.].

Brenner SW, Schwerha JJ. Cybercrime haven. The Computer & Internet Lawyer 2008;25(9):19−21.

Broadhurst R, Choo K-K R. Cybercrime and on-line safety in cyberspace. In: Smith C, Zhang S, Barberet R, editors. Routledge International Handbook of Criminology. NY: Routledge; 2011. p. 153–65.

Center for Strategic and International Studies (CSIS). Securing cyberspace for the 44th presidency. Washington, DC: Center for Strategic and International Studies; 2008.

Choo KKR. Zombies and botnets. Trends & issues in crime and criminal justice no. 333: 1–6, http://www.aic.gov.au/publications/current%20series/tandi/321-340/tandi333.aspx; 2007 [Date last accessed: 06.07.11.].

Choo KKR. Organised crime groups in cyberspace: a typology. Trends in Organized Crime 2008;11(3):270–95.

Choo KKR. Cloud computing: challenges and future directions. Trends & issues in crime and criminal justice no. 400: 1–6, http://www.aic.gov.au/publications/current%20series/tandi/381-400/tandi400.aspx; 2010 [Date last accessed: 06.07.11.].

Choo KKR. Cyber threat landscape faced by financial and insurance industry. Trends & issues in crime and criminal justice no. 408: 1–6, http://www.aic.gov.au/publications/current%20series/tandi/401-420/tandi408.aspx; 2011 [Date last accessed: 06.07.11.].

Choo KKR & Grabosky P forthcoming. Cyber crime. In Letizia Paoli, editor, Oxford Handbook of Organized Crime, New York: Oxford University Press.

Choo KKR, Smith RG, McCusker R. Future directions in technology-enabled crime: 2007–09. Research and public policy series no 78. Canberra: Australian Institute of Criminology, http://www.aic.gov.au/publications/current%2520series/rpp/61-80/rpp78.aspx; 2007 [Date last accessed: 06.07.11.].

Cohen LE, Felson M. Social change and crime rate trends: a routine activity approach. American Sociological Review 1979;44(4):588–608.

Conti G, Easterly J. Recruiting, development, and retention of cyber warriors despite an inhospitable culture. Small Wars Journal, http://smallwarsjournal.com/blog/journal/docs-temp/482-conti-easterly.pdf; 2010 [Date last accessed: 06.07.11.].

Dandurand Y, Colombo G, Passas N. Measures and mechanisms to strengthen international cooperation among prosecution services. Crime, Law and Social Change 2007;47(4–5):261–89.

Drummond D. A new approach to China. Google blog 12 January, http://googleblog.blogspot.com/2010/01/new-approach-to-china.html; 2010 [Date last accessed: 06.07.11.].

Falliere N, Murchu LO, Chien E. W32.Stuxnet dossier: Version 1.3. Cupertino, CA: Symantec; November 2010.

Federal Bureau of Investigation (FBI). Combating cyber crime: global network operates 24–7. Media release 14 January, http://www.fbi.gov/page2/jan09/fordham_011409.html; 2009 [Date last accessed: 06.07.11.].

Federal Bureau of Investigation (FBI). Manhattan U.S. attorney charges 37 defendants involved in global bank fraud schemes that used "zeus trojan" and other malware to steal millions of dollars from U.S. bank accounts. Media release 30 September, http://newyork.fbi.gov/dojpressrel/pressrel10/nyfo093010.htm; 2010 [Date last accessed: 06 07.11.].

Felson M. Crime and everyday life. New York: Pine Forge Press; 1998.

Glavin RG. Statement of Rita G Glavin, acting assistant attorney general criminal division united states department of justice before the house of representatives homeland security committee subcommittee on emerging threats, cybersecurity, and science & technology, http://www.justice.gov/criminal/cybercrime/glavinStatement.pdf; 2009 [Date last accessed: 06.07.11.].

Gjelten T. Volunteer cyber army emerges In Estonia, http://www.npr.org/2011/01/04/132634099/in-estonia-volunteer-cyber-army-defends-nation; 2011 [Date last accessed: 06.07.11.].

Goldman G. Government slideshow: Federal investment in cyber security to reach $13.3 billion by 2015. CIO insight 29 December, http://www.cioinsight.com/c/a/Government/Federal-Investment-in-Cyber-Security-to-Reach-133-Billion-by-2015-305281/; 2010 [Date last accessed: 06.07.11.].

Grabosky P. The internet, technology, and organized crime. Asian Journal of Criminology 2007;2(2):145–61.

Gross G. Mobile malware exploits on the way, experts say. CSO.com.au 6 October, http://www.cso.com.au/article/363341/mobile_malware_exploits_way_experts_say?eid=-302; 2010 [Date last accessed: 06.07.11.].

Ho PK. The 19th Governmentware Seminar at The Suntec Singapore International Convention & Exhibition Centre – Speech By Associate Professor Ho Peng Kee, Senior Minister Of State For Law & Home Affairs. Media release 28 September, http://www.mha.gov.sg/news_details.aspx?nid=MTg0OA%3d%3d-0J3MocXe%2bmU%3d; 2010 [Date last accessed: 06.07.11.].

HM Government. A strong Britain in an age of uncertainty: the national security strategy. Whitehall, London: The Stationery Office; 2010.

IBM X-Force®. IBM X-Force® 2010 trend and risk report. Somers, NY: IBM Corporation, http://public.dhe.ibm.com/common/ssi/ecm/en/wgl03007usen/WGL03007USEN.PDF; 2011 [Date last accessed: 06.07.11.].

Jakobsson M & Juels A 2009. Server-side detection of malware infection. In Proceedings of New Security Paradigms Workshop (NSPW 2009), pp. 11–29.

Kirk J. ATM malware spreading around the world. CIO.com 6 June, http://www.cio.com/article/494341/ATM_Malware_Spreading_Around_the_World; 2009 [Date last accessed: 06.07.11.].

Leyden J. Siberian crooks dev'd custom malware in ATM slurp heist scheme. The register 3 December, http://www.theregister.co.uk/2010/12/03/russian_atm_malware_scam/; 2010 [Date last accessed: 06.07.11.].

Lookout. Lookout mobile threat report: August 2011, https://www.mylookout.com/_downloads/lookout-mobile-threat-report-2011.pdf; 2011 [Date last accessed: 05.08.11.].

Markoff J. Worm can deal double blow to nuclear program. NYTimes 19 November, http://www.nytimes.com/2010/11/20/world/middleeast/20stuxnet.html?ref=technology; 2010 [Date last accessed: 06.07.11.].

McAfee. Virtual criminology report 2009: virtually here: the age of cyber warfare. Santa Clara, CA: McAfee 2009, Inc; 2009.

McGlasson L. Agencies issue ACH, wire fraud advisory. Govinfosecurity 15 March, http://www.govinfosecurity.com/articles.php?art_id=2298; 2010 [Date last accessed: 06.07.11.].

McMillan R. NSA helped Microsoft make vista secure. CSO 10 January, http://www.csoonline.com.au/index.php?id=2112787630&eid=-302; 2007 [Date last accessed: .06.07.11.].

McMillan R. Comerica bank ordered to pay after customer hacked. Computerworld 15 June, http://www.computerworld.com/s/article/9217662/Comerica_Bank_ordered_to_pay_after_customer_hacked?taxonomyName=Security&taxonomyId=17; 2011a [Date last accessed: 06.07.11.].

McMillan R. US Phisher Who Hit 38,500 Gets Long Prison Sentence. PC World 29 July, http://www.pcworld.com/businesscenter/article/236877/us_phisher_who_hit_38500_gets_long_prison_sentence.html; 2011b [Date last accessed: 03.08.11.].

Obama B. Remarks by the president on securing our nation's cyber infrastructure, http://www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure/; 2009 [Date last accessed: 06.07.11.].

Ponemon Institute. Second annual cost of cyber crime study: benchmark study of U.S. Companies. Michigan, USA: Ponemon Institute LLC; 2011.

Pras A, Sperotto A, Moura GCM, Drago I, Barbosa R, Sadre R, et al. Attacks by "Anonymous" WikiLeaks proponents not anonymous, http://www.geenstijl.nl/archives/images/loic-report.pdf; 2010 [Date last accessed: 06.07.11.].

Richards K. The Australian Business Assessment of Computer User Security: a national survey. Research and public policy No 102. Australian Institute of Criminology; 2009.

RSA. RSA online fraud report: September, 2010, http://www.rsa.com/solutions/consumer_authentication/intelreport/11094_Online_Fraud_report_0910.pdf; 2010 [Date last accessed: 06.07.11.].

Rudd K. Address by the Prime Minister of Australia The Hon. Kevin Rudd MP 4 December 2008, http://pmrudd.archive.dpmc.gov.au/node/5424; 2008 [Date last accessed:06.07.11.].

Sim SH. Effective countermeasures against economic crime and computer crime. Resource material series no. 55. Tokyo: United Nations Asia and Far East Institute for the Prevention of Crime and the Treatment of Offenders; 2000. 103–116.

Smith RG, Grabosky P, Urbas G. Cyber criminals on trial. Cambridge: Cambridge University Press; 2004.

Symantec. Symantec global internet security threat report: trends for 2009, Vol. XV; 2010, http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xv_04-2010.en-us.pdf; 2010 [Date last accessed: .06.07.11.].

Symantec. Symantec internet security threat report: trends for 2010, https://www4.symantec.com/mktginfo/downloads/21182883_GA_REPORT_ISTR_Main-Report_04-11_HI-RES.pdf; 2011 [Date last accessed: 06.07.11.].

Sydney Morning Herald (SMH). Most sophisticated mobile virus starts spreading on Android smartphones, http://www.smh.com.au/digital-life/mobiles/most-sophisticated-mobile-virus-starts-spreading-on-android-smartphones-20101231-19bne.html; 2010. SMH.com.au 31 December[Date last accessed: 06.07.11.].

US-China Economic and Security Review Commission 2009. 2009 report to congress. http://www.uscc.gov/annual_report/2009/annual_report_full_09.pdf [Date last accessed: 06.07.11.].

US-China Economic and Security Review Commission 2010. 2010 report to congress. http://www.uscc.gov/annual_report/2010/annual_report_full_10.pdf[Date last accessed: .06.07.11.].

Yar M. The novelty of 'cybercrime': an assessment in light of routine activity theory. European Journal of Criminology 2005; 2(4):407–27.

Since graduating with a Ph.D. in Information Security in September 2006, **Dr Kim-Kwang Raymond Choo** has (co-)authored a number of publications in information security, cyber crime and anti-money laundering including a book published in Springer's "Advances in Information Security" book series, three Australian Government Australian Institute of Criminology (AIC) refereed monographs, and several book chapters. He has served as an editorial board member for a number of international journals, program committee member for a number of international conferences, workshop/conference coordinator, and reviewer for a number of international conferences and journals in the areas of information security and cyber crime.