RESOURCE MATERIAL SERIES
No. 97

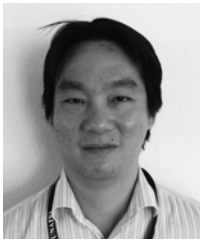
Work Product of the 160th International Training Course

"The State of Cybercrime: Current Issues and Countermeasures"

UNAFEI

CURRENT SITUATION AND MODI OPERANDI OF CYBERCRIME

*Dr. Kim-Kwang Raymond Choo**



I. CYBERSPACE: THE NEW FRONT LINE

As the majority of our business and general communication is currently being conducted over the Internet and our online presence increases, physical distance may no longer be an obstacle in conducting business transactions or reaching out to individual citizens. For example, the number of individuals now online is slightly over 3 billion since June 2014 and no doubt the numbers have increased since then.

World Internet Usage And Population Statistics (30 June 2014)						
World Regions	**Population (2014 Est.)**	**Internet Users Dec. 31, 2000**	**Internet Users Latest Data**	**Penetration (% Population)**	**Growth 2000-2014**	**Users % of Table**
Africa	1,125,721,038	4,514,400	**297,885,898**	26.5 %	6,498.6 %	9.8 %
Asia	3,996,408,007	114,304,000	**1,386,188,112**	34.7 %	1,112.7 %	45.7 %
Europe	825,824,883	105,096,093	**582,441,059**	70.5 %	454.2 %	19.2 %
Middle East	231,588,580	3,284,800	**111,809,510**	48.3 %	3,303.8 %	3.7 %
North America	353,860,227	108,096,800	**310,322,257**	87.7 %	187.1 %	10.2 %
Latin America / Caribbean	612,279,181	18,068,919	**320,312,562**	52.3 %	1,672.7 %	10.5 %
Oceania / Australia	36,724,649	7,620,480	**26,789,942**	72.9 %	251.6 %	0.9 %
WORLD TOTAL	**7,182,406,565**	**360,985,492**	**3,035,749,340**	**42.3 %**	**741.0 %**	**100.0 %**

Table 1: World internet usage and population statistics as of 30 June 2014 (Source: http://www.internetworldstats.com/stats.htm, last accessed 20 April 2015).

It is interesting to note that even though only about 35% of Asia's population has access to the Internet, this represents close to half of the world's current population with access to the Internet (see Table 1). Australia, on the other hand, has 72.9% of the population online, but this only represent 0.9% of the world's population and less than 2% of Asia's Internet population.

Our increased dependence on information and communications technologies (ICT) and cyberspace — also known as the fifth dimension of warfare/conflict (e.g. the US Department of Defense (2011: 5) considers 'cyberspace is now as relevant a domain for DoD activities as the naturally occurring domains of land, sea, air, and space'). The pervasive interconnectivity of systems used in our ICT-connected society are potential vectors that can be exploited by actors with malicious intents, ranging from cybercriminals acting alone to organized groups of financially, criminally and issue-/ideologically motivated crime groups to state sponsored actors.

This should not come as a surprise; and as Holt and Bossler (2013) explained, "[a]s technology increasingly permeates all facets of modern life, there are substantive risks to the safety of digital information

*Fulbright Scholar and Senior Researcher, University of South Australia, Australia.
Email: raymond.choo@unisa.edu.au. This paper is compiled from the author's previously published materials.

and computer networks". The increasing popularity of smart mobile devices (e.g. iOS and Android devices), for example, constitutes an opportunity for cybercriminals (Imgraben, Engelbrecht and Choo 2014).

Cybercrime is an emerging issue of growing concern for individuals, businesses, and governments (see Australian Government 2013), given the rapid development and proliferation of ICT. Cybercrime may not have the dramatic impact of a nuclear and/or kinetic military attack and/or result in mass casualties, but they can have serious effects on the present and/or future of defensive or offensive effectiveness of a country's national and cybersecurity.

Examples of short and long term impacts of cybercrime on their victims include:

Short-term impact

- Impacting the daily activities of individual end users (e.g. affecting their ability to receive up-to-date information about power grid shutdown due to an ongoing cyberattack, and carrying out online financial transactions and conducting other daily online activities); and

- 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;

- Social discontent and unrest (e.g. loss of public confidence in the government even if the actual damage caused by the malicious cyber-activities was minimal); and

- Loss of intellectual property, which can affect the long-term competitiveness of businesses and governments in industrial and military espionage incidents.

Notwithstanding the threat of a cyber-Armageddon, a greater problem resides in the capacity of smaller scale attacks on selected critical infrastructure sectors such as power grid networks, which could potentially overwhelm and paralyse the country's interconnected critical infrastructure sectors and, consequently, cause social unrest. For example, a coordinated cyber- and physical attack on a country/city's power grid networks using sophisticated malware (similar to Stuxnet and Flame) and improvised explosive devices could potentially cripple our transport system and other critical infrastructure systems (typically connected to the Internet). These attacks could have undesirable consequences such as equipment being forced to operate beyond their intended design and safety limits, resulting in cascading system malfunctions and shutdowns — see Box 1. Ensuring the resilience and high availability of communication channels where up-to-date situational information should be a key part of the government's civil contingency plans.

A hypothetical situation

CERT-In notified India's National Security Council Secretariat and the National Command Post that various government agencies and private sector organisations were under cyberattacks (e.g. coordinated attacks on systems by malware exploiting several zero-day vulnerabilities)

Consequences

Systems such as the following could potentially be affected, and consequently result in massive damages and loss to both property and human lives. For example, technical problems associated with computer-based despatch systems used by health and emergency services (e.g. ambulances) could potentially contribute to misadventures resulting in fatalities due to delayed or misdirected ambulances.

- Telecommunication infrastructure (including mobile communication)
- SCADA systems (e.g. compromising SCADA systems used in water treatment facilities or pumping stations could cause build-up of sewage posing health and hygiene risks, or causing inappropriate amounts of chemicals (particularly chlorine) in water treatment could result in unsafe drinking water or could pose environmental risks in sewage treatment).
- Traffic control systems (e.g. railway, road traffic control, and air traffic control)
- Oil refineries and chemical plants
- Banking and financial systems
- Health and emergency services
- Defence and other government systems

Box 1: A hypothetical cyberattack adapted from Choo (2010) and the Institute for Defence Studies and Analyses Task Force Report on India's cybersecurity challenge (Gupta, Singh, Bajaj, Srinath, Waris, Sharma, Lele, Samuel and Patil 2012, pp. 14–16).

II. MALICIOUS CYBER-ACTIVITY

A. Criminal or an Act of Cyberwar?

The intended effects of malicious cyber-activities include exfiltration of data and information (e.g. trade secrets and intellectual property), exploitation of vulnerabilities to execute malware, and disruption and denial of services; with the aims of disrupting one or more combinations of the following security (CIAA) notions:

- *Confidentiality* ensures that data are available only to authorised parties. To achieve this notion, encryption using mathematical algorithms is typically used to encrypt the data and render the encrypted data unintelligible to anyone else, other than the authorised parties even if the unauthorised party has access to the encrypted data.
- *Integrity* ensures that data have not been tampered with or modified. To achieve this notion, several approaches such as the use of a one-way cryptographic hash function together with encryption or use of a message authentication code (a key-based mathematical algorithm that allows two parties, who have shared a secret key in advance, to authenticate their subsequent communication), have been adopted to detect data manipulation such as insertion, deletion, and substitution. An example is the unauthorized modification of information used by governments, particularly those used by defence agencies, to spread the fear of an imminent terrorist attack and consequently causing social unrest.
- *Availability* ensures that data continue to be available at the minimal operational level in situations ranging from normal to disastrous.
- *Authentication* ensures the identification of either the data (data origin authentication) or the entity (entity authentication). Data origin authentication implicitly provides data integrity since the unauthorised alteration of the data implies that the origin of the data is changed, as the origin of data can only be guaranteed if the data integrity has not been compromised in any way. The use of a one-way cryptographic hash function together with encryption or use of a message authentication code can help to achieve data origin authentication. Entity authentication is a communication process by which a party establishes live correspondence with a second party whose identity should be that which is sought by the first party.

Malicious cyber-activities can be broadly categorised into cybercrime, cyberwar, cyberterrorism and cyberespionage (although there is no international consensus on these definitions — see Bendiek 2012;

ENISA 2012). For example, the term "cybercrime" is referred to in *Australia's Cybercrime Act 2001* (Cth) as well as the Council of Europe Convention on Cybercrime with different meanings. The Australian Government's Cyber Security Strategy "defines cybercrime as those computer offences under the Commonwealth Criminal Code Act 1995 (Part 10.7) that involve unauthorised access to, modification or impairment of electronic communications" (e.g. hacking, malware intrusions and denial of service attacks) (Australian Government Attorney-General's Department 2009: 23).

Cybercrime has also been defined by various other researchers and organisations to reflect activities where ICT are the targets of the act (against both the private sector, such as cloud service providers (Higgins 2014), and nation states, such as the attacks against Estonia in 2007 (Rid 2012) and the more recent attacks against South Korea (Leyden 2013)) and acts where ICT are integral to the criminal or harmful behaviour (such as online fraud against individuals, businesses, and/or government agencies, online child/young-people sexual exploitation (e.g. online child grooming), cyber-bullying, and cyber-stalking).

Investigating and prosecuting cross-border cybercrime cases can be extremely challenging without the cooperation of the international community, as the nature of cyberspace enables criminals to exploit sovereignty issues and cross-jurisdictional differences. In addition, successfully tracking the digital trail requires quick and co-ordinated action between agencies and across borders but the costs of such investigations and prosecutions can be very expensive.

If we are able to make the distinction whether an incident is criminal or an act of cyberwar, we would be in an informed position to identify the appropriate response to each of the threats (e.g. who is best placed to respond and what are the rules of engagement). Unfortunately, as explained by Choo and Grabosky (2014), it has not been an easy task trying to distinguish between criminally motivated and state-sponsored cyberattacks in all cases or to find the smoking gun.

Governments may not use civil servants to perform their dirty work. They can turn a blind eye to malicious cyber-activities that are seen as serving state interests, or offer active encouragement to cybercriminals. This could be partly due to the lack of a legal definition of cyberwarfare or agreement on what constitutes an act of war in cyberspace. For example, if attacks against another country cannot be committed legally using conventional forces, some governments have a strong incentive to covertly sponsor cybercriminals rather than overtly engaging in such activities without suffering the political and legal consequences.

B. Examples of Existing and Emerging Threat Vectors

Whether a malicious cyber-incident is criminal or an act of war, malware (malicious software) is often used to compromise consumer technologies (see Section B.2) and devices such as mobile devices (see Section B.1) by exploiting vulnerabilities in the hardware and software that we use. The threat of malware is not really new. However, malware has consistently been ranked as one of the key cyberthreats to businesses, governments and individuals over the past few years (Choo 2011). Recent statistics such as those of Cisco (2014), Symantec (2015) and Verizon (2015) and studies of D'Orazio and Choo (2015), Do, Martini and Choo (2015) and Zhou and Jiang (2015) have indicated a steady increase in the number of new malware and the number of vulnerabilities in the commercial off-the-shelf hardware and software each year, as well as the potential for these vulnerabilities to be criminally exploited. Malware can be broadly categorized into (a) generic malware that targets the general population and (b) customized information-stealing malware targeting specific institutions. An example of a generic malware is bot malware designed to exploit particular vulnerabilities on mobile devices of individual end users, businesses and governments (Choo 2007).

1. Mobile Devices and Mobile Applications

Mobile devices and applications (or apps, as they are commonly known) are an important tool for accessing information when desktop computers and laptops are unavailable. These devices are used to perform phone-specific tasks such as texting and making phone calls as well as other tasks, such as web browsing and internet banking. For example, a study of 4,125 mobile device users in 2011 found that an average mobile user spent approximately 59.23 minutes per day on their mobile devices, and the average app session is approximately 71.56 seconds (Böhmer et al. 2011), and a report by Gartner (2013) forecasts that by 2017, approximately 86% of devices shipped worldwide will be running one of the four major mobile

operating systems, namely Android, iOS, Windows Phone and BlackBerry.

Due to the capability of mobile devices and apps to access sensitive data and personally identifiable information (PII), such as medical history and electronic health transactions, they present a genuine security and privacy threat to their users. In the rush to attract new consumers and accelerate the product's time-to-market, many mobile apps were not designed with user security and privacy in mind. For example, the active location broadcast added to many popular apps are of security and privacy concerns, as with sufficiently accurate location data, it is possible to determine a user's address, track their movements and even stalk a user throughout the day (Cheung 2014).

As remarked by D'Orazio and Choo (2015), this situation is similar to twenty or thirty years ago when cryptographic protocols were routinely published without a rigorous security analysis and, subsequently, found to be insecure. For example, the study conducted by Hewlett Packard (2013) revealed that 90% of the 2,107 mobile apps examined were vulnerable to attacks, and 97% accessed sensitive data and PII and 86% had privacy-related risks. Another more recent report released by Alcatel-Lucent (2015)

> 'estimate[d] that worldwide, about 16 million mobile devices are infected by malware … Android phones and tablets are responsible for about 50% of the malware infections observed. Currently most mobile malware is distributed as "Trojanized" apps and Android offers the easiest target for this because of its open app environment.

Therefore, it is not surprising that mobile apps have attracted the attention of security researchers. For example, D'Orazio and Choo (2015) revealed a previously unknown / unpublished vulnerability in a widely used Australian Government healthcare app, which would allow a cybercriminal to obtain access to the user's sensitive data and PII such as claim history and electronic health transactions stored on the affected iOS device.

In another recent work, Do, Martini and Choo (2015) demonstrate how sensitive data and PII can be obtained from Android devices in a covert manner using communication mediums, such as SMS and audio, found on almost all mobile devices. The inaudible exfiltration technique demonstrated by the authors had been shown to be effective in collecting passwords and encryption keys using only a standard microphone (such as those on another smartphone). Also noted by the authors, their attacks have the potential to affect a range of different applications and mobile device user communities.

Malicious cyber-activities targeting mobile devices and apps will continue to evolve into new forms, while continuing to exploit human factors (e.g. social engineering), and human factors are likely to remain one of the weakest links in attempts to secure mobile devices and apps. Encouraging users to be more proactive about protecting their data is always a good approach, and allowing users to choose their own level of privacy ensures that they are comfortable with the information they are sharing.

However, studies have highlighted that most mobile device and app users may not be aware of the security and privacy implications of sharing their information (Felt, Egelman and Wagner 2012). A survey of 250 mobile device owners from the University of South Australia (UniSA), for example, found that the participants generally underestimated cybercriminal risks and the value that their collective identities have to criminals and how these can be sold (Imgraben, Engelbrecht and Choo 2014).

Users inherently place value on their own data, but value different types of data differently, and may place more value on specific data at certain times or at certain locations. A user may not care about their location data being shared if they benefit from sharing it, such as a taxi driver being tracked to ensure his/her safety, but would probably not want his/her employer tracking his/her every movement when he/she is not working as the latter would be considered an invasion of a user's privacy. The increasingly popular dating apps, for example, encourage the sharing of more personal information than conventional social media apps, including continuous location data. However, recent high profile incidents, such as targeted robbery and sexual assault cases (Koubaridis 2014; Wilson 2014), have highlighted the privacy risks inherent in using dating apps. Dating apps as well as those that collect geo-location data can also be used to profile a user, and many users upload documents or photos that have location data attached without realizing the extent of information they are sharing.

Cheung (2014) explains that it may also be against privacy laws to collect this data as a user never agrees to give his/her full consent for most location sharing. While there has been some research on understanding the security and privacy risks of social network check-ins, the implications of more active (aggressive) location tracking such as proximity-based dating or "hook-up" apps have not been fully explored, but have been shown to be vulnerable to collusion attacks (Farnden, Martini and Choo 2015; Fattori *et al.* 2013).

There are several challenges in designing malware prevention solutions, such as anti-malware solutions, for mobile devices. For example, anti-malware solutions that are efficient for traditional computing systems may not be suitable for deployment on a mobile device due to software and hardware constraints, etc. Real time protection against malware threats will often adversely affect the device's performance and battery life. Users may also not be diligent in keeping the anti-malware signature up-to-date or ignoring specific alerts. The effectiveness of anti-malware solutions utilizes signature definitions to detect malware threats. Depending on the accuracy and up-to-date malware signature definitions, known malware threats may go undetected — this is a known limitation of the signature-based detection system.

Another challenge involves third-party app stores, which allow mobile-device and app users to download and install an app on their device. The majority of third-party app stores have their own app submission guidelines, if any. For example, the Amazon App Store requires Android app developers to submit their apps through an approval and guidelines system, where they are vetted prior to release. However, third-party app stores are unlikely to have an equally stringent process in place. Thus, given the open source nature of Android, apk files may be re-packaged with malicious code and submitted to third-party app stores without approval guidelines.

The challenge is compounded by careless and uneducated mobile device users who may not understand the potential risks associated with installing apps that request excessive or unnecessary permissions (Imgraben, Engelbrecht and Choo 2014). Although there are a number of resources explaining permissions, such as the Android permissions model, there is a risk of how certain permissions work together, such as app communication and cross-app interaction. In addition, mobile device users have no easy way of determining whether a particular anti-malware app is effective.

2. Cloud

The term cloud computing refers to a model whereby a user can access computing resources via a network on an on-demand basis (Mell and Grance 2011). Various types of resources can be shared between users and in a way that remote clients can utilise them, e.g. processing, volatile and persistent storage and so on. This pool of resources is commonly available as a service via an internal network (private cloud) or publically via the Internet (public cloud). In addition to providing the de facto definition of cloud computing, the National Institute of Standards and Technology (NIST) also defined a number of service models including: Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS) (Mell and Grance 2011).

Storage as a Service (STaaS) is an addition to these traditional service models. STaaS technologies enable users to store, download and share their data in a very accessible manner. There are a number of STaaS service providers including Dropbox, Microsoft OneDrive, Google Drive and Ubuntu One. These service providers commonly provide personal accounts for minimal or no cost. Cloud service providers (CSPs) have made significant efforts to attract customers by supporting various types of devices ranging from traditional computing platforms such as Windows, Mac OS X and Linux to more recent mobile device operating systems such as iOS and Android. Also, CSPs generally offer access to their services via standards compliant web browsers including Internet Explorer, Google Chrome, Mozilla Firefox and Apple Safari. These features allow users to access their data via the majority of Internet connected devices.

As noted by a number of researchers (Martini, Do and Choo 2015; Quick, Martini and Choo 2014; Shariati et al. 2015), while cloud services provide legitimate users with significant utility and convenience, they are equally useful to criminals who utilize them for storing and sharing illicit materials.

Therefore, to keep pace with the growth and changing face of criminal activity, CSPs and users, particularly organizational users, must have a model that they can use to identify, classify, quantify, and priori-

tize threats and risk. Juliadotter and Choo (2015a, 2015b) studied some 21 existing attack taxonomies for traditional computing systems published between January 2003 and April 2014, and based on the review, proposed a cloud attack and risk assessment taxonomy designed to facilitate the identification of attack risk element and, therefore, minimizing loss to cloud service providers and users in the event of a cyberattack.

The dimensions of Juliadotter and Choo's (2015a) attack taxonomy follow the natural flow of an attack on a cloud service. The taxonomy's top level comprises five dimensions: source, vector, target, impact, and defense. For example, in a security incident, identifying the attack's source or the attacker will facilitate our understanding of the taxonomy's second level: context, motivation, opportunities, and skill level.

III. THE WAY AHEAD: A THREE-PRONGED CYBERCRIME MITIGATION APPROACH

Ensuring the security of our cyber-future is defined not only by human, process and technical perfection but rather by an ability to manage these imperfections; and should be a shared responsibility between the public sector, private actors and the community (Choo 2014).

To ensure the country's long-term national security and competitiveness, government agencies including law enforcement agencies have a primary responsibility to make detailed preparations to act against current and emerging threats against the country before it is too late, as well as to recover from a wide range of malicious cyber-activities when they succeed (resilience). A cybercrime mitigation approach — see Figure 1 — should be dynamic and be regularly reviewed by stakeholders. Such an approach is somewhat similar to the practice of intelligence analysis, which involves a continuous cycle of tasking, collection, collation, analysis, dissemination and feedback (Ratcliffe 2003).

Only by working in collaboration with the industry, research community and international partners (though *proactive partnership* and *proactive engagement*) can we begin to tackle existing and emergent cyberspatial threats (identified during the *environment scan*) as it would allow us to better address the knowledge and research gaps in the existing evidence base and contribute to the strategic, operational and policy vacuum; and help to ensure that developments in technologies, political, geographical, socioeconomic, legal and regulatory, etc are well understood and can be used to refine policy strategies (e.g. setting of

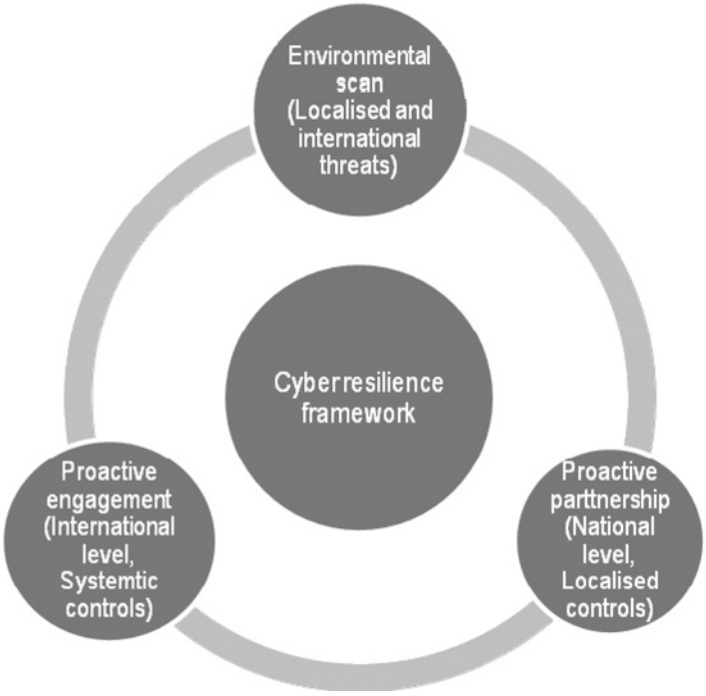


Figure 1: Conceptual cybercrime mitigation approach

resource priorities). Such an approach also aligns with the strategy put forward in a recent report prepared for the Canadian Security Intelligence Service (Gendron and Rudner 2012), which highlighted the importance of (1) identifying existing and emergent threats, a partnership approach, and the role of intelligence; and the Australian Government Critical Infrastructure Resilience Strategy, which emphasised the importance of (1) sector and cross-sector engagement as well as international engagement, and (2) managing unforeseen or unexpected risk through intelligence and information led, risk informed and organisational resilience approach approaches (Australian Government Attorney-General's Department 2010).

A. Environmental Scan (Localised and International Threats)

An environmental scan would include a review of current information on the cybersecurity threat as cyberthreats, and windows of vulnerability evolve over time, partly in response to defensive actions or crime displacement. It is also essential to canvass global developments of the criminal, political, regulatory and business environments that may give rise to malicious cyber-activities, as, clearly, many of the risks are based in global features of the criminal economy and the global threat landscape.

Although the speed of change in ICT development and adoption means that history may offer limited guidance about the future threat landscape, understanding the threat landscape is crucial to a country's national and cybersecurity agenda.

B. Proactive Partnership (National Level, Localised Controls)

A cybercrime mitigation doctrine based on offensive actions are unlikely to work, and it would be rather unlikely for governments to resort to large-scale hostile or military cyber-retaliation simply on the basis of the *cui bono* logic or circumstantial evidence. A Colonel in the US Army who directs the International Relations Program in the Department of Social Sciences at the US Military Academy at West Point, for example, suggested that "In the case of the nuclear standoff between the United States and the Soviet Union, deterrence was both cheaper and more technically feasible than defense. However, it is questionable whether deterrence can play a significant role in current U.S. cybersecurity policy" (Nielsen 2012, p. 352). A similar observation was raised in the report prepared for the US-China Economic and Security Review Commission — "[e]ven if circumstantial evidence points to China as the culprit, no policy currently exists to easily determine appropriate response options to a large scale attack on U.S. military or civilian networks in which definitive attribution is lacking" (Krekel, Adams and Bakos 2012, p. 9).

An effective cybercrime mitigation strategy requires policies and objectives that align with stakeholder needs, coupled with strong political commitment. For example, the United Nations Guidelines for the Prevention of Crime state that the basic principles for prevention of crime is to have government leadership, cooperation / partnerships, a broad and multidisciplinary foundation of knowledge about issues, causes and evidence-based practices, etc (UN ECOSOC 2002). Senior stakeholders in both public and private sectors need to understand the importance of the right governance enablers and more importantly, to understand that cybercrime mitigation and cybersecurity are not only a cost or an ICT issue, but it can facilitate economic exchange and deliver real business benefits.

C. Proactive Engagement (International Level, Systemic Controls)

ICT create various interdependencies between key sectors, with many of the same technology-related risks affecting one or more of these sectors and in more than one country, and potentially lead to larger-scale and often unanticipated failures. In addition, the interdependencies may also result in mutual dependence between sectors and countries and complicate recovery efforts.

Therefore, the oversight and governance of critical infrastructure resilience should involve all key stakeholders in the public sector, private sector and the research community at both the national and international levels. A proactive partnership will also result in collaboration and strategic alliances outside our borders for critical infrastructure resilience and help us to identify and prioritise current and emerging risk areas (including risk arising from unexpected and highly unpredictable causes — also known as the "black swan" problem), and hence, achieving systemic resilience.

As Gary Lewis, UNODC Regional Representative for East Asia and the Pacific, emphasised "[c]ooperation between law enforcement agencies and with the information and communication technology (ICT) sector is essential. Let us not forget that in fighting [organised criminal] network, we ourselves also consti-

tute a network. It may sound corny to say this, but it takes a network to defeat a network" (UNODC 2011). The 2011 revised NATO Policy on Cyber Defence "sets out a clear vision of how the Alliance plans to bolster its cyber efforts" (NATO 2011, p. 1), which includes "work[ing] with partners, international organisations, academia and the private sector in a way that promotes complementarity and avoids duplication" (NATO 2011, p. 2). Similar observations have been echoed by other political observers and scholars such as Nielsen (2012).

It can be extremely challenging for stakeholders operating within a dynamic/real-time environment to immediately evaluate whether a cyberthreat situation has occurred, assess the risks and act upon the assessment. Accuracy and effectiveness of the response can be broadly seen as a function of resources (including time) and expertise and understanding of the threat landscape, and how the threat impacts on interconnected systems in other sectors. Therefore, to facilitate the sharing and dissemination of timely and actionable cyber-alerts, classified or sensitive information, and research findings (e.g. vulnerabilities or zero-day exploits discovered by researchers), it is essential to establish secure and trusted information-sharing mechanisms among the public sector, private sector and the research community outside of the hierarchist confines of typical government initiatives.

This would enable all parties involved to produce threat assessments based on fresh and accurate information; and to develop a collaborative, real-time, and active cyber-capability to detect, analyze, and mitigate malicious cyber-activities that would hopefully stop malicious cyber-incidents in progress and minimize the damage, as well as to facilitate the investigation of cross-border malicious cyber-incidents. However, establishing a secure mechanism to share information, particularly classified and sensitive information, within government agencies and between sectors both domestically and internationally is challenging. An audit report by the US Government Accountability Office (2013: 53), for example, found that "the [US] federal government continues to face challenges in effectively sharing threat and incident information with the private sector and in developing a timely analysis and warning capability".

If we are able to determine the most cost-effective way to bridge the gap between sectors and countries, we would be able to better address any disconnect between them. Consequently, all stakeholders involved will find it much easier to collectively contribute to the strategic, operational and policy vacuum and ensure that global developments are well understood and can be used to refine policy strategies.

References

Alcatel-Lucent 2015. *Kindsight security labs malware report – H2 2014*. <https://resources.alcatel-lucent.com/asset/184652> [last accessed 20 April 2015]

Australian Government 2013. *Strong and secure: A strategy for Australia's national security*. Canberra, ACT: Commonwealth of Australia

Australian Government Attorney-General's Department 2009. *Cyber security strategy*. ACT, Australia: Commonwealth of Australia

Australian Government Attorney-General's Department 2010. Critical infrastructure resilience strategy. ACT, Australia: Commonwealth of Australia. <http://www.tisn.gov.au/Documents/Australian+Government+s+Critical+Infrastructure+Resilience+Strategy.pdf> [last accessed 20 April 2015]

A. Bendiek A 2012. European cyber security policy. *SWP Research Paper 13*, Berlin, Germany: German Institute for International and Security Affairs

M. Böhmer, B. Hecht, J. Schöning, A. Krüger, and G. Bauer 2011. Falling asleep with Angry Birds, Facebook and Kindle: A large scale study on mobile application usage. In Proceedings of the 13th International Conference on Human Computer Interaction with Mobile Devices and Services, 30 August – 2 September, Stockholm, Sweden, pp. 47–56.

A. S. Y. Cheung 2014. Location privacy: The challenges of mobile service devices. *Computer Law & Security Review*, vol. 30, no. 1, pp. 41–54.

K.-K. R. Choo 2007. Zombies and botnets. *Trends & Issues in Crime and Criminal Justice*, vol. 333, pp. 1–6.

K.-K. R. Choo 2010. High tech criminal threats to the national information infrastructure. *Information Security Technical Report*, vol. 15, no. 3, pp. 104–111.

K.-K. R. Choo 2011. Cyberthreat landscape faced by financial and insurance industry. *Trends & Issues in Crime and Criminal Justice*, vol. 408, pp. 1–6.

K.-K. R. Choo 2014. A conceptual interdisciplinary plug-and-play cyber security framework. In H. Kaur and X. Tao, editors, ICTs and the Millennium Development Goals – A United Nations Perspective, pp. 81–99, New York, USA: Springer.

K.-K. R. Choo and P. Grabosky 2014. Cyber crime. In L.a Paoli, editor, Oxford Handbook of Organized Crime, pp. 482–499, New York: Oxford University Press.

Cisco 2014. Cisco 2014 annual security report. San Jose, CA: Cisco Systems, Inc.

C. D'Orazio and K.-K. R. Choo 2015. A generic process to identify vulnerabilities and design weaknesses in iOS healthcare apps. In Proceedings of the 48th Hawaii International Conference on System Sciences, 5–8 January, Kauai, Hawaii, USA, pp. 5175–5184.

Q. Do, B. Martini, and K.-K. R. Choo 2015. Exfiltrating data from Android devices. *Computers & Security*, vol. 48, pp. 74–91.

European Network and Information Security Agency (ENISA) 2012. *National cyber security strategies: Setting the course for national efforts to strengthen security in cyberspace*. <http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/cyber-security-strategies-paper/at_download/fullReport> [last accessed 20 April 2015]

J. Farnden, B. Martini, and K.-K. R. Choo 2015. Privacy risks in mobile dating apps. In Proceedings of 21st Americas Conference on Information Systems (AMCIS 2015), 13–15 August 2015, Puerto Rico [In press].

A. Fattori, A. Reina,; A. Gerino, and S. Mascetti. On the privacy of real-world friend-finder services. In Proceedings of IEEE International Conference on Mobile Data Management (MDM 2013), 3–6 June 2013, Milan, Italy, pp. 331–334.

A. Gendron, and M. Rudner 2012. *Assessing cyber threats to Canadian infrastructure: Report prepared for the Canadian Security Intelligence Service*. <http://www.csis-scrs.gc.ca/pblctns/cdmctrch/20121001_ccsnlpprs-eng.asp> [last accessed 1 April 2014]

A. P. Felt, S. Egelman, and D. Wagner 2012. I've got 99 problems, but vibration ain't one: a survey of smartphone users' concerns. In Proceedings of the Second ACM Workshop on Security and Privacy in Smartphones and Mobile Devices (SPSM 2012), 16–18 October 2012, NC, USA, pp. 33–44.

Gartner 2013. *Gartner says worldwide pc, tablet and mobile phone combined shipments to reach 2.4 billion units in 2013*. <http://www.gartner.com/newsroom/id/2408515> [last accessed 20 April 2015]

A. Gupta, A. Singh, K. Bajaj, B.J. Srinath, S. Waris, A. Sharma A, A. Lele, C. Samuel, and K. Patil 2012. *India's cyber security challenge*. New Delhi, India: Institute for Defence Studies

J. Hagmann, and M. D. Cavelty 2012. National risk registers: Security scientism and the propagation of permanent insecurity. *Security Dialogue*, vol. 43, no. 1, pp. 79–96.

Hewlett-Packard 2013. *HP research reveals nine out of 10 mobile applications vulnerable to attack*.

<http://www8.hp.com/us/en/hp-news/press-release.html> [last accessed 20 April 2015]

K. J. Higgins 2014. Wave of DDoS attacks down cloud-based services. *Dark Reading*, 6 November. <http://www.darkreading.com/attacks-breaches/wave-of-ddos-attacks-down-cloud-based-services/d/d-id/1269614> [last accessed 20 April 2015]

T. J. Holt and A. M. Bossler 2013. Examining the relationship between routine activities and malware infection indicators. *Journal of Contemporary Criminal Justice*, vol. 29, no. 4, pp. 420–436.

J. Imgraben, A. Engelbrecht, and K.-K. R. Choo 2014. Always connected, but are smart mobile users getting more security savvy? A survey of smart mobile device users. *Behaviour & Information Technology*, vol. 33, no. 12, pp. 1347–1360.

N. V. Juliadotter, and K.-K. R. Choo 2015a. Cloud attack and risk assessment taxonomy. *IEEE Cloud Computing*, vol. 2, no. 1, pp. 14–20.

N. V. Juliadotter, and K.-K. R. Choo 2015b. Conceptual cloud attack taxonomy and risk assessment framework. In R. Ko and K.-K. R. Choo, editors, Cloud Security Ecosystem, Syngress, an Imprint of Elsevier [In press]

A. Koubaridis 2014. Tourist sexually assaulted in Sydney by several men after meeting on Tinder. *News.com.au*, 8 October. <http://www.news.com.au/national/tourist-sexually-assaulted-in-sydney-by-several-men-after-meeting-on-tinder/story-fncynjr2-1227083995690> [last accessed 4 May 2015]

B. Krekel, P. Adam, and G. Bakos 2012. *Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage*. http://origin.www.uscc.gov/sites/default/files/Research/USCC_Report_Chinese_Capabilities_for_Computer_Network_Operations_and_Cyber_%20Espionage.pdf [Last accessed 5 May 2015]

J. Leyden 2013. South Korean TV and banks paralysed in disk-wipe cyber-blitz. *The Register*, 20 March. <http://www.theregister.co.uk/2013/03/20/south_korea_cyberattack/> [last accessed 20 April 2015]

B. Martini, Q. Do and K.-K. R. Choo 2015. Mobile cloud forensics: An analysis of seven popular Android apps. In R. Ko and K.-K. R. Choo, editors, Cloud Security Ecosystem, Syngress, an Imprint of Elsevier [In press]

North Atlantic Treaty Organization (NATO) 2011. *Defending the networks: The NATO policy on cyber defence*. <http://www.nato.int/nato_static/assets/pdf/pdf_2011_08/20110819_110819-policy-cyberdefence.pdf> [Last accessed 5 May 2015]

S. C. Nielsen 2012. Pursuing security in cyberspace: Strategic and organizational challenges. *Orbis Summer*, vol. 2012, pp. 336–356.

D. Quick, B. Martini and K.-K. R.Choo 2014. *Cloud storage forensics*. Syngress, an Imprint of Elsevier.

J. Ratcliffe 2003. Intelligence-led policing. *Trends & Issues in Crime and Criminal Justice*, vol. 248, pp. 1–6.

T. Rid 2012. Cyber war will not take place. *Journal of Strategic Studies*, vol. 35, no. 1, pp. 5–32.

M. Shariati, A. Dehghantanha, B. Martini and K.-K. R. Choo 2015. Ubuntu One Investigation: Detecting Evidences on Client Machines. In R. Ko and K.-K. R. Choo, editors, Cloud Security Ecosystem, Syngress, an Imprint of Elsevier [In press]

Symantec 2015. 2015 internet security threat report. Mountain View, CA: Symantec

US Department of Defense 2011. Department of Defense strategy for operating in cyberspace. <http://www.defense.gov/news/d20110714cyber.pdf> [last accessed 20 April 2015]

United Nations Economic and Social Council (UN ECOSOC) 2002. Guidelines for the prevention of crime. 11th Commission on the prevention of crime and criminal justice. Resolution 2002/13, Annex. New York: UN ECOSOC.

United Nations Office on Drugs and Crime (UNODC) 2011. *Asia-Pacific acts to counter cybercrime*. <http://www.unodc.org/southeastasiaandpacific/en/2011/09/cybercrime-workshop/story.html> [Last accessed 5 May 2015]

US Government Accountability Office 2013. *Cybersecurity: National strategy, roles, and responsibilities need to be better defined and more effectively implemented*. GAO-13-187, Washington, DC: United States Government Accountability Office

Verizon 2015. *2015 data breach investigations report*. <http://www.verizonenterprise.com/DBIR/2015/> [last accessed 20 April 2015]

Wilson, L. 2014. Warriena Tagpuno Wright murder: Does Tinder leave you exposed? *News.com.au*, 15 August. <http://www.news.com.au/technology/online/warriena-tagpuno-wright-murder-does-tinder-leave-you-exposed/story-fnjwnhzf-1227025983590> [Last accessed 4 May 2015].

Zhou, Y. and Jiang, X. 2012. Dissecting Android malware: Characterization and evolution. In Proceedings of 2012 IEEE Symposium on Security and Privacy, 21–23 May 2012, San Francisco, California, USA, pp. 95–109.