RESOURCE MATERIAL SERIES No. 97

UNAFEI

Fuchu, Tokyo, Japan

December 2015

YAMASHITA Terutoshi
Director

United Nations
Asia and Far East Institute
for the Prevention of Crime and
the Treatment of Offenders
(UNAFEI)

1-26 Harumi-cho, Fuchu, Tokyo 183-0057, Japan
http://www.unafei.or.jp
unafei@moj.go.jp

CONTENTS

WORK PRODUCT OF THE 160TH INTERNATIONAL TRAINING COURSE

"THE STATE OF CYBERCRIME: CURRENT ISSUES AND COUNTERMEASURES"

Visiting Expert's Papers

Participants' Papers

Reports of the Course

INTRODUCTORY NOTE

It is with pride that the United Nations Asia and Far East Institute for the Prevention of Crime and the Treatment of Offenders (UNAFEI) offers to the international community the Resource Material Series No. 97. This volume contains the work product of the 160th International Training Course, conducted from 13 May to 17 June 2015. The main theme of the 160th International Training Course was *The State of Cybercrime: Current Issues and Countermeasures*.

On 23 November 2001, 30 countries, including Japan, signed the Convention on Cybercrime. The Convention aimed to counter cybercrime by harmonizing criminal legislation and establishing closer international cooperation. Nevertheless, criminal justice practitioners from developed and developing countries alike still face numerous challenges in the investigation and prosecution of cybercrime. These challenges include rapidly changing technology, the anonymity of cybercriminals and the borderless nature of cybercrime.

UNAFEI, as one of the institutes of the United Nations Crime Prevention and Criminal Justice Programme Network, held this Course to explore various issues that relate to cybercrime. This issue of the *Resource Material Series* contains papers contributed by one of the visiting experts, selected individual-presentation papers from among the participants, and the Reports of the Course. I regret that not all the papers submitted by the participants of the Course could be published.

I would like to pay tribute to the contributions of the government of Japan, particularly the Ministry of Justice, the Japan International Cooperation Agency, and the Asia Crime Prevention Foundation, for providing indispensable and unwavering support to UNAFEI's international training programmes. Finally, I would like to express my heartfelt gratitude to all who so unselfishly assisted in the publication of this series.

December 2015

YAMASHITA, Terutoshi

YAMASHITA, Terutoshi
Director of UNAFEI

RESOURCE MATERIAL SERIES
No. 97

Work Product of the 160th International Training Course

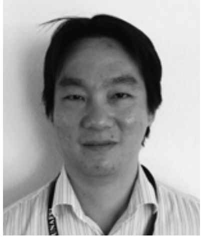
“The State of Cybercrime: Current Issues and Countermeasures”

UNAFEI

VISITING EXPERT'S PAPERS

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. <u>Mobile Devices and Mobile Applications</u>

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 prioritize 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

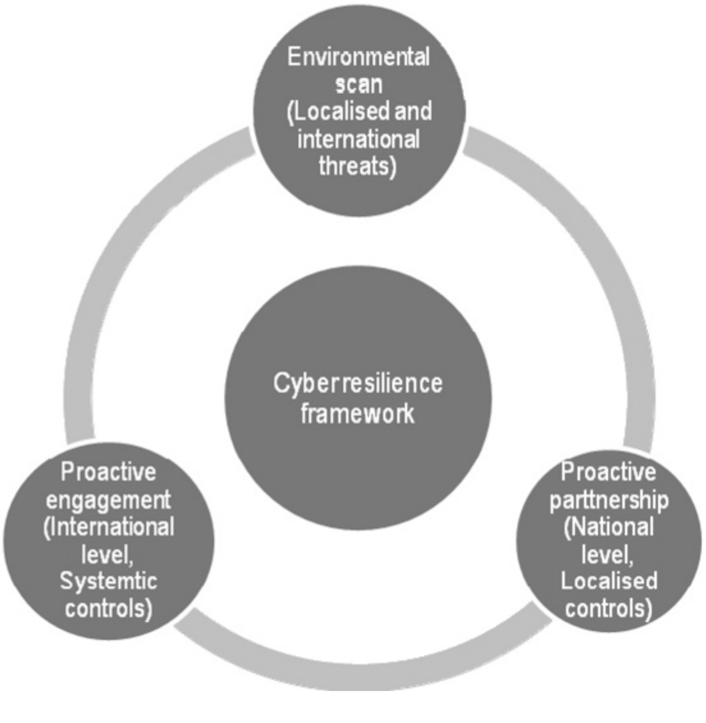

Environmental scan (Localised and international threats)
Cyberresilience framework
Proactive engagement (International level, Systemtic controls)
Proactive parttnership (National level, Localised controls)

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 constitute 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

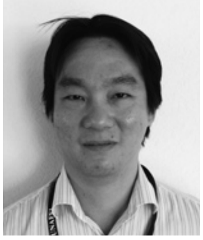
Verizon 2015. *2015 data breach investigations report.* <http://www.verizonenterprise.com/DBIR/2015/> [last accessed 20 April 2015]

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.

CONTEMPORARY DIGITAL FORENSIC INVESTIGATIONS

Dr. Kim-Kwang Raymond Choo[*]



I. DIGITAL FORENSIC INVESTIGATIONS

Information and communications technologies (ICT) are fundamental to modern society and open the door to increased productivity, faster communication capabilities, and immeasurable convenience. However, the era of ICT-enhanced globalisation has also been accompanied by an increase in the sophistication and volume of malicious cyber-activities. Malicious cyber-activities are a rapidly expanding form of criminality that knows no borders, and such activities can have serious effects on the present and/or future of defensive or offensive effectiveness of a country's national and cybersecurity. The consequences can impact a vast array of sectors, including fixed and mobile telecommunications, traffic control systems, water treatment facilities, health and emergency services, defence and other government systems and much more (see Choo 2010b).

Given the increase in ICT (e.g. cloud services, mobile devices and Internet-of-Things) in everyday life, digital evidence is becoming more commonplace. However, attempting to gather digital evidence from a range of systems and devices, particularly across borders, resulted in new challenges for government and law enforcement agencies. The former South Australian Director of Public Prosecutions explained that "[f]or the prosecutor, the challenge is to have the data translated into a form that is acceptable as evidence to the courts ... Assuming that the fragile and elusive evidence can be gathered together, the prosecutor must keep in mind that he or she will one day need to be able to prove the chain of evidence. All processes will need to be appropriately documented in a way that can be understood by the layman, and the prosecutor must be prepared if necessary to demonstrate that the 'original' digital material has not been changed or tampered with in any way" (Pallaras 2011: 80). Such a process is known as digital forensics, and is increasingly being used in the courts in Australia and overseas. It is, therefore, important to have a rigorous methodology and set of procedures for conducting digital forensic investigation as well as incident response.

Digital forensics, a relatively new sub-discipline of forensic science when compared to other common forensic science disciplines, is the process of gathering evidence of some type of an incident or crime that has involved computer systems and their associated networks (see McKemmish 1999; Martini and Choo 2012; Quick, Martini and Choo 2014). In such circumstances, the expectation is that there has been some accumulation or retention of data by the various components of a system which will need to be identified, preserved and analysed. This process can be documented and defined, and be used to obtain information or evidence pertaining to a crime or malicious cyber-incident. For example, when the systems belonging to a cloud service provider are compromised, digital forensics can be used to facilitate the collection of evidence from compromised cloud servers and client devices for analysis. This would allow subsequent reconstructing of the incident and establish facts such as

- Where did the attack come from?;
- What vulnerability(ies) was/were exploited?; and
- What data / which systems was/were compromised? (Ab Rahman and Choo 2015).

[*]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, including those co-authored with Nurul Hidayah Ab Rahman, Abdullah Afzar, Andrew Butler, Quang Do, Jody Farnden, Lin Liu, Ben Martini and Darren Quick.

The evidence collected can be used to inform risk mitigation strategy as well as be used in the prosecution of the offender in a court of law. To ensure the admissibility of evidence in a court of law, it is necessary to identify and examine the many influences, impacts upon and contributions to the presentation of evidence by an expert witness. Suffice to note that for an expert witness to provide their opinion there must be forensic evidence that requires interpretation and presentation, and for forensic evidence to exist, an investigative process would need to have been undertaken in response to an incident, criminal or civil (Butler and Choo 2015).

McKemmish (1999, p. 1) provided one of the first definitions of digital forensics, defining it as: "the process of identifying, preserving, analysing and presenting digital evidence in a manner that is legally acceptable". There are four key elements in McKemmish's digital forensics framework — namely, the identification, preservation, analysis and presentation of digital evidence.

1. Identification of digital evidence defines the requirement for evidence management, knowing it is present, its location and its type and format.

2. Preservation is concerned with ensuring evidential data remains unchanged or changed as little as possible. For example, if a forensic investigator needs to recover data from a device, it is important that the data is recovered using methods that are forensically sound (e.g. they do not write to the original data source as information such as 'file last accessed times' on key system files could be changed if a seized computer is improperly booted before a disk image capture is undertaken).

3. Analysis transforms the bit level data collected in the earlier two phases into evidence presentable to a court of law.

4. Finally, the presentation element is concerned with presenting evidence to the courts in terms of providing expert testimony on the analysis of the evidence.

As noted by Martini and Choo (2012), another widely used digital forensics framework is that of the National Institute of Standards and Technology (NIST) (Kent et al. 2006). The four phases and definitions in NIST's framework share some similarities with the framework of McKemmish (1999):

1. Collection discusses identifying relevant data, preserving its integrity and acquiring the data;

2. Examination uses automated and manual tools to extract data of interest while ensuring preservation;

3. Analysis is concerned with deriving useful information from the results of the examination; and

4. Reporting is concerned with the preparation and presentation of the forensic analysis (Kent et al. 2006, p. ES-1).

II. CLOUD AND MOBILE FORENSICS

Due to the increasing popularity of consumer devices such as mobile devices and technologies such as cloud computing, existing forensic frameworks may not be fit-for-purpose. For example, existing digital forensic techniques are designed to collect evidential data from devices where we have physical access or from typical mobile device users (e.g. where advanced security features and anti-forensic techniques are rarely exploited to their full extent). In contrast, serious and organised criminals often make use of devices specifically designed to evade legal interception and forensic collection attempts. In the case of cloud forensics, Bagby and Schwerha (2013) also raised a number of legal questions, such as the physical location of records. As noted by the authors, "subpoenas used by investigators as well as the document production demands made in civil litigation generally require accurate physical location data for targeted files, backups, responsible custodians (humans), and knowledgeable supervisors" (Bagby and Schwerha 2013, p. 13).

Therefore, the digital forensic "space" can be seen as a race, not only to keep up with device (i.e.

hardware) and software releases by providers (e.g. cloud service provider and mobile app designers), but also from software and hardware modifications made by end users, particularly serious and organised criminals, to complicate or prevent the collection and analysis of digital evidence.

A. Cloud Forensics

The growth in the use of cloud computing has resulted in a growing need for forensic investigations involving cloud technologies and, consequently, spawned the growth of research in cloud forensics (Martini and Choo 2014). The lack of physical access to digital artefacts over the servers spanning across multiple jurisdictional areas as well as integrity of data artefacts (e.g. log files) provided by the Cloud Service Providers (CSP) (Chung et al 2012; Grispos, Storer, and Glisson 2013; Hooper, Martini, and Choo 2013; Martini and Choo 2014a) complicate digital investigations. Even if the evidence could be identified, it could be illegal to access the raw log data that contains records of multiple users in a multi-tenancy cloud environment (ENISA, 2012). The wide range of mobile devices (Zatyko and Bay 2011; Tassone et al. 2013) and the use of encryption by CSPs or individuals (Grispos, Storer, and Glisson 2012) further complicate cloud forensic investigations.

In recent years, researchers have attempted to extract evidential data from data remnants on client devices when a cloud storage service has been accessed on these devices. For example, Chung et al. (2012) analyzed Amazon S3, Google Docs and Evernote and, based on the findings, presented a plan to collect data from personal computers and mobile devices. Hale (2013) studied Amazon cloud drive on Windows XP and Windows 7 computers.

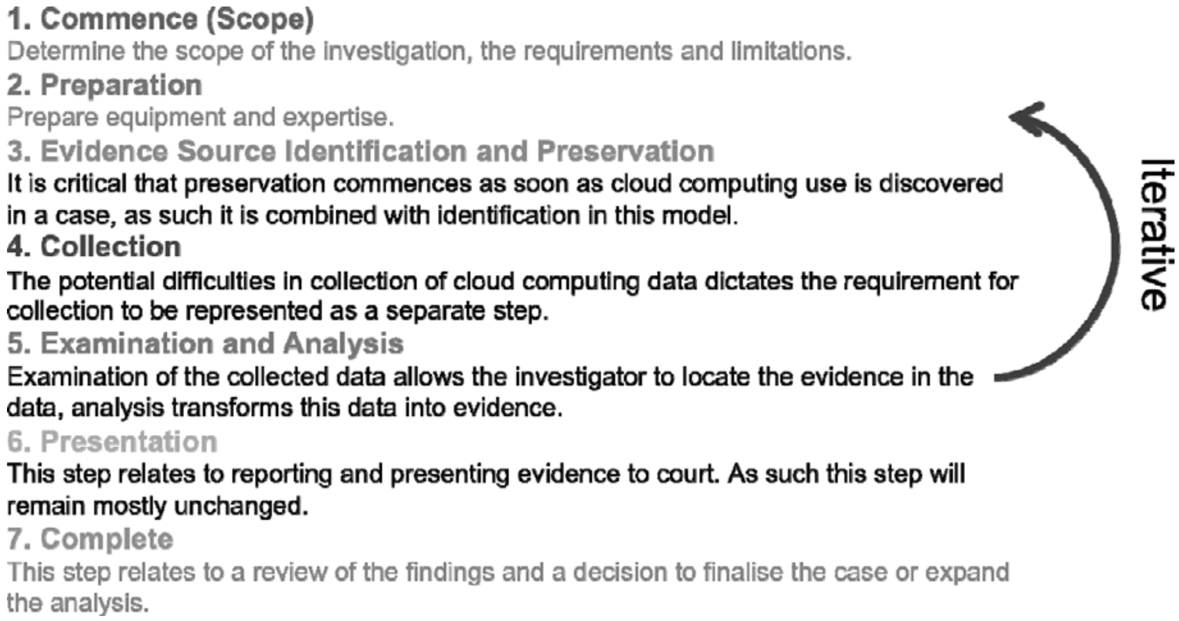
The first digital forensic framework designed for both client and server investigations of cloud services is presented by Martini and Choo (2012). The framework, based on McKemmish (1999) and NIST (Kent et al. 2006), has been validated by the authors using ownCloud (Martini & Choo 2013), XtreemFS (a distributed filesystem) (Martini & Choo 2014b), and vCloud (Martini & Choo 2014c), as well as by Thethi and Keane (2014) using EC2 cloud. There are four stages in this framework, namely: evidence source identification and preservation, collection, examination and analysis, and reporting and presentation for collecting digital evidence from the cloud environment — see Table 1.

1. Evidence Source Identification and Preservation. In this phase, potential sources of relevant data are identified. Any device capable of connecting to the cloud services, either via a browser or a client application, is considered a potential source of evidence. In this phase, the investigator should also ensure that ACPO principles are adhered to, wherever possible.

2. Collection. During collection of evidence from storage media, particularly media belonging to external parties, the investigator should also ensure that relevant laws and regulations are followed (Kent et al. 2006).

3. Examination and Analysis. Information from acquired data is extracted in this phase. Methods to circumvent or bypass protection mechanisms on the devices may be used to examine and analyze information collected and preserved from the previous phase (e.g. use of tools to brute-force password-protected data). During this phase, findings should also be reviewed with information or intelligence drawn from other sources and investigations before a conclusion is drawn.

4. Presentation. In the last phase, findings are documented for presentation in a court of law.



1. Commence (Scope)

Determine the scope of the investigation, the requirements and limitations.

2. Preparation

Prepare equipment and expertise.

3. Evidence Source Identification and Preservation

It is critical that preservation commences as soon as cloud computing use is discovered in a case, as such it is combined with identification in this model.

4. Collection

The potential difficulties in collection of cloud computing data dictates the requirement for collection to be represented as a separate step.

5. Examination and Analysis

Examination of the collected data allows the investigator to locate the evidence in the data, analysis transforms this data into evidence.

6. Presentation

This step relates to reporting and presenting evidence to court. As such this step will remain mostly unchanged.

7. Complete

This step relates to a review of the findings and a decision to finalise the case or expand the analysis.

Figure 1: Integrated cloud forensic framework of Quick, Martini and Choo (2014)

Another cloud forensic framework was proposed a year later by Quick and Choo (2013a) and validated using Dropbox (Quick and Choo 2013b), SkyDrive (Quick and Choo 2013a) and Google Drive Quick and Choo (2014). These two frameworks were subsequently merged into one (Quick, Martini, Choo 2014) — see Figure 1.

In the integrated framework, the process is iterative as it is common that during an investigation a forensic practitioner may need to return to a previous phase. For example, during the examination and analysis phase, a practitioner may uncover information relating to data stored with a particular CSP. The practitioner may start a new iteration of the framework and undertake enquiries to locate, identify, and collect the newly identified data using legal processes. At the same time, the forensic analysis of other data already collected would continue. Once the CSP has been identified, the investigator or the practitioner will commence preservation and collection of the data.

Table 1: Summary of cloud forensic challenges (Ab Rahman and Choo 2015)

Cloud	Challenges	Service(s) affected	Potential mitigation strategies	References
Multi-tenancy (Virtualised environment)	Confidentiality and privacy issue of data belonging to or about cloud service users (CSUs) residing on the same physical machine but are not part of the law enforcement investigation or court orders	SaaS , PaaS, IaaS (slightly)	Virtual machine (VM) snapshots can serve as the acquisition image; traditional forensic acquisition may need to be adapted; digital forensics readiness; standard event information format; Information disclosure policy Potential research topic: Remote cloud forensics	(Grobauer & Schreck 2010); (Monfared & Jaatun 2012); (Zimmerman & Glavach 2011)
	Cloud service provider (CSP) may have difficulties in specifically referring to the malicious or compromised VM, due to resource pooling	IaaS		
	Different log formats due to different hardware used, and challenges in segregating log files of CSUs not under investigation	SaaS, PaaS, IaaS		
Multi-location (i.e. data location)	Complications due to time synchronisation as data is likely to reside on multiple physical machines in multiple geographical regions with different time zones	SaaS, PaaS, IaaS	Harmonised regulation and compliance; improving log generation technique to allow successful analysis and correlation of information from varying sources; improving live analysis techniques; international protocol to achieve time synchronisation (e.g. RFC 5095); digital forensics readiness	(Grobauer & Schreck 2010); (Zimmerman & Glavach 2011); (Martini & Choo 2012)
	Data mirroring over multiple machines in different jurisdictions, lack of transparency, and non-uniform privacy and related laws	SaaS, PaaS, IaaS		
	CSP may not be able to provide a precise physical location of the data location	SaaS, PaaS, IaaS		
Scope of user control (and cloud actors participation)	Logging and log details are heavily dependent on CSP: CSU has no or limited access to event sources and vulnerability information generated by infrastructure components under the control of CSP	SaaS, PaaS	● Granular configuration of functionality and access rights; and must be clarified in SLA ● Client-side incident response and forensic investigation can be conducted for IaaS and PaaS ● CSP should provide a set of security APIs (e.g. event monitoring, forensic services, IDS/IPS, policy-based autonomic management system) as add-on services, or implementing middleware tool ● CSP can implement software agent on CSU's site to facilitate a cross-layer security solution; therefore neither CSU nor CSP need to know each other's architecture. ● Incident detection and reporting obligations (e.g. Amazon Vulnerability Report, ENISA Cloud Incident Reporting Framework), and must be set out in SLA ● More attention to mutual auditability ● Dedicated monitoring tool and policy of cloud insider incident.	(Grobauer & Schreck 2010); (Monfared & Jaatun 2012); (Kozlovszky et al. 2013); (Sarkar et al. 2011); (Li et al. 2012); (Dekker, Liveri & Lakka 2013)
	Inability to add security-specific event sources (e.g. web application firewall)	SaaS, PaaS		
	No or limited knowledge about architecture	SaaS (mostly), PaaS		
	Unclear incident handling responsibilities among cloud stakeholders	SaaS, PaaS, IaaS		
	Data ownership — deleted data, terminated contract, CSP shuts down business.	SaaS, PaaS, IaaS		
	Participation of a few number of CSPs, e.g. a CSP that provides an email application (SaaS) may depend on a third-party provider to host log files (PaaS)	SaaS (mostly), PaaS, IaaS		
	Requires a specific strategy for incident handling	SaaS (mostly), PaaS, IaaS (slightly)		
	CSP's employee (insider) may compromise security and privacy of CSU	SaaS (mostly), PaaS, IaaS (slightly)		
	Lack of coordination or interruption of activities correlation (dependency chain) across cloud stakeholders	SaaS (mostly), PaaS, IaaS		
	Misdirection of incident reporting (to whom should reports be directed?)	SaaS, PaaS, IaaS		

B. Mobile Forensics

Evidential information that can be potentially extracted from a mobile device includes SMS messages, phone call logs, photos and location data. While extraction of these types of data has been commonplace for some time, more recently a focus has been placed upon collecting data from third-party apps that users install on their mobile devices. In a recent work, for example, Azfar, Choo and Liu (2015) examine 40 popular Android mobile health apps. Based on their findings, a taxonomy incorporating artefacts of forensic interest to facilitate the timely collection and analysis of evidentiary materials is proposed — see Table 1.

App Name	Version	App Category				Artefact Category						
		Patient care and monitoring	Health apps for the layperson	Communication, education, and research	Physician or student reference	Databases	User credentials and pins	Personal details of users	User activities	User location	Activity timestamps	Images
MyFitnessPal	3.6.1	P	F	P	N	F	P	F	F	N	F	F
RunKeeper - GPS	5.4	N	F	N	N	F	N	N	F	F	F	N
Period Calendar	1.51	P	F	N	N	F	F	F	F	N	P	N
WebMD	3.5	N	F	F	P	P	N	N	P	N	N	N
Blood Pressure (BP) Watch	3.0.11	P	F	N	N	F	N	P	F	N	F	N
Calorie Counter by FatSecret	-	P	F	P	N	F	N	N	F	N	P	N
Google Fit	1.51.07	N	F	N	N	P	N	N	P	N	F	N
MyNetDiary Calorie Counter PRO	2.2.0	P	F	P	N	N	N	N	N	N	N	F
Drugs.com Medication Guide	1.23	N	F	F	P	F	N	F	N	N	P	N
My Diet Diary Calorie Counter	1.9.11	P	F	P	N	F	N	P	F	N	F	N
Calories! Basic – cal counter	1.1.7	P	F	P	N	F	N	N	P	N	F	N
Period Tracker	2.0.6.4	P	F	N	N	F	N	N	F	N	P	N
Calorie Counter	4.2.5	P	F	P	N	F	N	F	F	N	F	N
My Pregnancy Today	1.14.0	P	F	N	N	N	P	N	N	N	N	F
Water Your Body	3.062	N	F	N	N	F	N	N	F	N	N	N
Instant Heart Rate	-	P	F	N	N	F	N	N	N	N	N	N
Calm – Meditate, Sleep, Relax	1.9.4	N	P	N	N	F	N	F	N	N	F	N
Runtastic Pedometer	1.5.1	N	F	N	N	F	N	N	F	N	F	N
Smiling Mind	2.0.3	N	F	N	N	F	N	F	N	N	F	N
Pedometer	5.10	N	F	N	N	P	N	N	F	N	F	N
Quit Now: My QuitBuddy	2.1	P	F	N	N	N	N	N	N	N	N	F

App Name	Version	App Category				Artefact Category						
		Patient care and monitoring	Health apps for the layperson	Communication, education, and research	Physician or student reference	Databases	User credentials and pins	Personal details of users	User activities	User location	Activity timestamps	Images
Mindbody Connect	2.8.3	N	P	N	N	F	N	N	P	P	N	N
My Baby Today	-	N	F	N	N	F	N	F	N	N	P	N
Lifesum- Calorie Counter	-	P	F	P	N	F	N	P	F	N	F	F
Quit Smoking – QuitNow!	-	N	F	N	N	N	N	N	N	N	N	N
Strava Running and Cycling GPS	4.3.1	N	F	N	N	F	N	F	F	F	F	N
Lorna Jane	1.2	N	F	N	N	F	N	N	P	F	F	F
Walk with Map My Walk	3.5.1	N	F	N	N	F	N	F	F	F	F	P
FitNotes – gym Workout Log	1.12.0	P	F	N	N	F	N	N	F	N	P	N
Nike+ Running	1.5.2	N	F	N	N	F	N	F	F	N	F	F
30 day Ab Challenge	2.0	N	P	N	N	N	N	N	N	N	N	N
Genesis YNB	1.0.2	N	F	N	N	N	N	F	N	P	N	F
BMI Calculator	-	N	P	N	N	N	N	N	N	N	N	N
Endomondo Running Cycling Walking	10.6.3	N	F	N	N	F	N	N	F	F	F	F
Fitness Buddy: 300+ Exercises	3.10	N	F	N	N	F	N	N	F	N	F	N
My Tracks	2.0.9	N	F	N	N	F	N	N	F	F	F	N
Under Armour Record	2.1.1	N	F	N	N	F	N	F	F	N	F	F
Noom Walk Pedometer: Fitness	1.1.0	N	P	N	N	F	N	N	F	N	F	F
Bleep Fitness Test	1.8	N	P	N	N	F	N	F	F	N	P	N
BodySpace- Social Fitness	1.3.9	N	F	N	N	F	N	F	F	N	P	F

Notes: "F" - detailed information was recovered; "P" - only partial information was recovered (e.g. artefacts from some apps provided partial timestamp such as only the date of the activity rather than the time in hours, minutes and seconds); and "N" - unsupported category.

Table 1: Mobile health app forensic taxonomy (Azfar, Choo and Liu 2015)

However, there has not been a commensurate level of research conducted on the most effective method of collecting and analyzing evidence from mobile apps. Much of the research (Barmpatsalou et al. 2013) which has been conducted in this area has also aged, as mobile devices and apps continue to advance and change with new mobile devices and apps being released on a regular basis.

Current digital forensics techniques for extracting data from a mobile device can be categorized into live analysis where the forensic information is taken directly from the device, and offline analysis where a copy of the device's data is analyzed (Martini, Do and Choo 2015a). However, existing research does not generally use a forensic framework as the basis of their evidence collection and/or analysis techniques.

Therefore, to contribute towards filling the literature gap, Martini, Do and Choo (2015a) present an evidence collection and analysis methodology for Android devices, which is designed to comply with forensic soundness principles, particularly in terms of data handling, and that the process is device agnostic as far as practical. The utility of the methodology is then demonstrated using seven popular Android cloud-based apps (Martini, Do and Choo 2015b) and nine popular Android mobile dating apps (Farnden, Martini and Choo 2015). Dating apps are a previously understudied app category that makes significant use of a user's location when the user checks-in, such as with Facebook and Foursquare, or uses a more active proximity system, where a user's location is continuously broadcast to find nearby users or locations.

Dating apps have come into public focus as popular dating sites, such as Plenty of Fish, are now reporting that 70% of usage takes place via a mobile phone. A study of the homosexual community found that many gay men surveyed had used mobile phones and a GeoSocial app (Phillips et al., 2014) to facilitate casual meetings. This is not surprising when Grindr, a popular gay dating GSN, has millions of users and continues to grow daily (Grov et al., 2014).

Despite all the hype and attention to dating apps, these services remain relatively understudied in traditional academic research, mainly being studied and analyzed only by enthusiasts. There is also limited support by professional forensic tools used by law enforcement and government agencies (e.g. EnCase, XRY, LANTERN, Paraben device seizure and ACESO), with most tools focusing on the more traditional address book and call log data. This inhibits the process of evidence collection, which is undertaken when a crime involving one or more of these apps is reported.

In the study of Farnden, Martini and Choo (2015), they determined that "[d]ating apps store messages or location readings on the device that can be used to reconstruct events or prove an alibi, which may aid in the prosecution of crimes involving these apps. In many cases, activities performed on the dating app could expose other members of the community, such as in the Grindr database, where there is a collection of all profiles the user has seen nearby, and the Skout app, which collected Facebook data from non-Skout users. In two cases (i.e. the FullCircle and MiuMeet apps), private images were viewable, which could be exploited by a malicious actor and this is a clear violation of user privacy".

III. THE WAY FORWARD

Contemporary digital forensics, particularly extracting data from remote cloud systems and devices that provide advanced security not only for data at rest (which has now become commonplace across all smart mobile devices) but also advanced encryption capabilities for data in transit (such as instant messages and emails being transmitted and received from a mobile device management (MDM) server), is an under-researched topic.

Current forensic techniques make use of vendor data communication facilities built into the mobile devices (e.g. iTunes backups for iOS devices) for the purpose of forensic extraction. Often this limits the potential for data extraction, for example, current tools would not be able to collect evidence from devices that are encrypted using strong passwords. A mobile computing device, such as a BlackBerry, which has been configured securely is almost impossible to analyze using current prevalent forensic techniques. Challenges faced by the digital forensic community are compounded when anti-forensic techniques are added to a device via software/hardware manufacturers or individual device users.

Therefore, it is important that research efforts be focused on contributing to filling the knowledge gap between existing scholarship and challenges faced by digital forensic practitioners and researchers (including those in governments) in this rapidly changing environment by addressing the following research questions:

1. How ICT are used in the commission and execution of serious and organized crimes, and how suspects are using advanced security features on systems and devices as well as anti-forensic techniques to evade legal forensic collection attempts?

2. What types of evidential data (e.g. data-at-rest and data-in-transit) are available, considering the

advanced security features and anti-forensic techniques that could be utilised by serious and organised criminals?

3. What techniques can government and law enforcement agencies use to legally gain access to the identified evidential data by circumventing advanced security features (e.g. developing low-level exploits and undertaking physical hardware analysis), without compromising the evidence's integrity?

To keep pace with the growth and changing face of criminal activity, particularly to ensure that evidential data can be forensically recovered, a number of governments have undertaken measures to enhance their technical capability (and in some instances, seeking to circumvent or weaken existing security measures) and introduce legislation that allows national security and law enforcement agencies to conduct online surveillance. For example, in September 2014, Australian government agencies have successfully lobbied for new legal powers to put Internet users under surveillance (see National Security Legislation Amendment Bill (No. 1) 2014).

Legitimate surveillance by government agencies (e.g. law enforcement, criminal intelligence and national security agencies) can be an effective crime deterrence measure, gather evidence, monitor the behaviour of known offenders and reduce the fear of crime. For example, analysis of intelligence gathered from different or disparate data sets (including data from the cloud and big data applications) may facilitate the prediction of major impending events and identify connections between individuals of interest.

Due to the advancement of ICT and interconnectedness of our society, however, the scope and reach of online surveillance by governments is constantly being expanded and sometimes to the detriment of individual privacy. For example, when we upload to or store our data (e.g. photos, videos and documents) in one of the cloud services, do we know the path of the transmitted data (i.e. through which countries or internet service providers our data will be routed) or whether anyone is collecting and analysing our transmitted or stored data?

While there is a legitimate need for cooperation between cloud service providers and governments, there are also concerns about cloud service providers being compelled to scan or search data of interest to 'national security' and to report on, or monitor, particular types of transactional data (Choo 2010a). Concerns about wide-scale government surveillance targeting cyberspace and invasion of individual user data privacy are not restricted to authoritarian societies but also liberal democracies, particularly post-11 September 2001. In 2013, for example, leaked US National Security Agency (NSA) documents by Edward Snowden, a former NSA contractor, indicated that the agency allegedly undertook broad online surveillance activities. The latter includes intercepting and collecting information from non-US citizens (as well as US citizens if they are conversing with a foreign target) and targeting organizations such as major US cloud computing service providers (Gellman and Lindeman 2014; Greenwald 2014).

In response to the NSA surveillance revelations, the European Parliament conducted an inquiry on the impact of the surveillance programme on European Union (EU) citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs. It was determined that these programmes allowed for the mass surveillance of internet users "through direct access to the central servers of leading US internet companies (PRISM programme), the analysis of content and metadata (Xkeyscore programme), the circumvention of online encryption (BULLRUN), access to computer and telephone networks, and access to location data, as well as to systems of the UK intelligence agency GCHQ such as the upstream surveillance activity (Tempora programme), the decryption programme (Edgehill), the targeted 'man-in-the-middle attacks' on information systems (Quantumtheory and Foxacid programmes) and the collection and retention of 200 million text messages per day (Dishfire programme)" (European Parliament 2014, p. 20).

The concern is generally not about the privacy rights of criminals or terrorist suspects, but the unintended collateral damage where the privacy of innocent individuals and ordinary citizens may be comprised in such surveillance programmes (e.g. finer granulated aspects of an individual's life are derived or inferred from the intelligence collection and analysis).

There is, therefore, a need to ensure that we balance the need for a secure cyberspace and the rights of individuals to privacy against the need to protect the community from serious and organized crimes and cybersecurity interests. This is an issue that has serious implications on the ability of governments to protect their citizens against serious and organized crimes. However, this remains an under-researched area perhaps due to the interdisciplinary challenges specific to this topic. Therefore, to develop theoretical clarity with real world applicability, it is important to bring together approaches from social science and computing to address the major contemporary forensic challenges associated with the use of securely configured ICT in serious and organised crimes.

References

N. H. Ab Rahman, and K.-K. R. Choo 2015. A survey of information security incident handling in the cloud. *Computers & Security*, vol. 49, pp. 45–69.

A. Azfar, K.-K. R. Choo, and L. Liu 2015. Forensic taxonomy of popular Android mHealth apps. In Proceedings of 21st Americas Conference on Information Systems (AMCIS 2015), 13–15 August 2015, Puerto Rico [In press].

J. W. Bagby, and J. J. Schwerha 2013. Migrating digital forensics and electronic discovery into the cloud: An injustice risk analysis. <http://faculty.ist.psu.edu/bagby/Pubs/ALSB2013_0103_paper.pdf> [Last accessed 5 May 2015].

K. Barmpatsalou, D. Damopoulos, G. Kambourakis, and V. Katos 2013. A critical review of 7 years of mobile device forensics. *Digital Investigation*, vol. 10, no. 4, pp. 323–349.

A. Butler, and K.-K. R. Choo 2015. IT standards and guides do not adequately prepare IT practitioners to appear as expert witnesses: An Australian perspective. *Security Journal* [In press, DOI: <http://dx.doi.org/10.1057/sj.2013.29>].

K.-K. R. Choo 2010a. Cloud computing: Challenges and future directions. *Trends & Issues in Crime and Criminal Justice*, vol. 400, pp. 1–6. <http://www.aic.gov.au/media_library/publications/tandi_pdf/tandi400.pdf> (Accessed October 2014).

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

H. Chung, J. Park, S. Lee, and C. Kang 2012. Digital forensic investigation of cloud storage services. *Digital Investigation*, vol. 9, no. 2, pp. 81–95.

M. Dekker, D. Liveri, and M. Lakka 2013. *Cloud security incident reporting framework for reporting about major cloud security incidents*. Heraklion, Greece: European Network and Information Security Agency.

European Network and Information Security Agency (ENISA) 2012. *Procure secure: a guide to monitoring of security service levels in cloud contracts*. Heraklion, Greece: European Network and Information Security Agency.

European Parliament 2014. Report on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs. <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A7-2014-0139+0+DOC+PDF+V0//EN> [Last accessed 5 May 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].

B. Gellman, and T. Lindeman. Inner workings of a top-secret spy program. *NYTimes* (29 June 2014). <http://apps.washingtonpost.com/g/page/national/inner-workings-of-a-top-secret-spy-program/282/> [Last accessed 5 May 2015].

G. Greenwald 2014. XKeyscore: NSA tool collects 'nearly everything a user does on the internet'. *The Guardian* (31 July 2013). <http://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data> [Last accessed 5 May 2015].

C. Grobauer, and T. Schreck 2010. Towards incident handling in the cloud. In Proceedings of the 2010 ACM Workshop on Cloud Computing Security Workshop (CCSW 2010), 8 October 2010, Chicago, IL, USA, pp. 77–85.

C. Grov, A. S. Breslow, M. E. Newcomb, J. G. Rosenberger, and J. A. Bauermeister 2014. Gay and bisexual men's use of the internet: Research from the 1990s through 2013. *The Journal of Sex Research*, vol. 51, no. 4, pp. 390–409.

G. Grispos, T. Storer, and W. Glisson 2012. Calm before the storm: the challenges of cloud computing in digital forensics. *International Journal of Digital Crime and Forensics*, vol. 4, no. 2, pp. 28–48.

J. S. Hale 2013. Amazon cloud drive forensic analysis. *Digital Investigation*, vol. 10, no. 3, pp. 259–265.

C. Hooper, B. Martini, and K.-K. R. Choo 2013. Cloud computing and its implications for cybercrime investigations in Australia. *Computer Law & Security Review*, vol. 29, no. 2, pp.152–163.

K. Kent, S. Chevalier, T. Grance, and H. Dang 2006. *Guide to integrating forensic techniques into incident response*. SP800-86, U.S. Department of Commerce, Gaithersburg.

M. Kozlovszky, L. Kovacs, M. Torocsik, G. Windisch, S. Acs, D. Prem, G. Eigner, P. Sas, T. Schubert, and V. Póserné 2013. Cloud security monitoring and vulnerability management. In Proceedings of the 17th IEEE International Conference on Intelligent Engineering Systems (INES 2013), 19–21 June 2013, San Jose, Costa Rica, pp. 265–269.

H. Li, X. Tian, W. Wei, and C. Sun 2012. A deep understanding of cloud computing security security issues in cloud computing. *Communications in Computer and Information Science*, vol. 345, pp 98–105.

R. McKemmish 1999. What is forensic computing? *Trends and Issues in Crime and Criminal Justice*, vol. 118, pp. 1–6.

B. Martini, and K.-K. R. Choo 2012. Cloud forensic technical challenges and solutions: A snapshot. *IEEE Cloud Computing*, vol. 1, no. 4, pp. 20–25.

B. Martini, and K.-K. R. Choo 2014a. An integrated conceptual digital forensic framework for cloud computing. *Digital Investigation*, vol. 9, no. 2, pp. 71–80.

B. Martini, and K.-K. R. Choo 2014b. Distributed filesystem forensics: XtreemFS as a case study. *Digital Investigation*, pp.1–19.

B. Martini, and K.-K. R. Choo 2014c. Remote programmatic vCloud Forensics: A six-step collection process and a proof of concept. In Proceedings of the 13th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom 2014), 24–26 September 2014, Beijing, China, pp. 935–942.

B. Martini, Q. Do, and K.-K. R. Choo 2015a. Conceptual evidence collection and analysis methodology for Android devices. In R. Ko and K.-K. R. Choo, editors, Cloud Security Ecosystem, Syngress, an Imprint of Elsevier [In press].

B. Martini, Q. Do, and K.-K. R. Choo 2015b. 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].

A. Monfared, and M. G. Jaatun 2012. Handling compromised components in an IaaS cloud installation.

Journal of Cloud Computing: Advances, Systems and Applications, vol. 1, no. 1, pp. 1–21.

S. Pallaras 2011. New technology: opportunities and challenges for prosecutors. *Crime, Law and Social Change*, vol. 56, no. 1, pp. 71–89.

G. Phillips, M. Magnus, I. Kuo, A. Rawls, J. Peterson, Y. Jia, J. Opoku, and A. E. Greenberg 2014. Use of geosocial networking (GSN) mobile phone applications to find men for sex by men who have sex with men (MSM) in Washington, DC. *AIDS and Behavior*, vol. 18, no. 9, pp. 1630–1637.

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

D. Quick, and K.-K. R. Choo 2013a. Digital droplets: Microsoft SkyDrive forensic data remnants. *Future Generation Computer Systems*, vol. 29, no. 6, pp. 1378–1394.

D. Quick, and K.-K. R. Choo 2013b. Dropbox analysis: Data remnants on user machines. *Digital Investigation*, vol. 10, no. 1, pp. 3–18.

D. Quick, and K.-K. R. Choo 2013c. Forensic collection of cloud storage data: Does the act of collection result in changes to the data or its metadata? *Digital Investigation*, vol. 10, no. 3, pp. 266–277.

Quick, D., & Choo, K.-K. R. (2014). Google Drive: Forensic analysis of data remnants. *Journal of Network and Computer Applications*, vol. 40, pp. 179–193.

C. Tassone, B. Martini, K.-K. R. Choo, and J. Slay 2013. Mobile device forensics: A snapshot. *Trends & Issues in Crime and Criminal Justice*, vol. 460, pp. 1–7.

N. Thethi, and A. Keane 2014. Digital forensics investigations in the cloud. In Proceedings of the 2014 IEEE International Advance Computing Conference (IACC 2014), 21–22 February 2014, Gurgaon, India, pp. 1475–1480.

K. Zatyko, and J. Bay 2011. The digital forensics cyber exchange principle. *Forensic Magazine*. <http://www.forensicmag.com/articles/2011/12/digital-forensics-cyber-exchange-principle> [last accessed 4 May 2015].

S. Zimmerman, and D. Glavach 2011. Cyber forensics in the cloud. *IAnewsletter*, vol. 14, no. 1, pp. 4–7.

THE STATE OF CYBERCRIME: CURRENT ISSUES AND COUNTERMEASURES

*Joash Dache, MBS**

I. INTRODUCTION

That the world has seen remarkable transformation with the advent of internet-based activities cannot be overemphasized[1]. This is because goods and services are routinely purchased and delivered electronically, leading to significant changes in various industries like journalism, travel, and banking. Significantly, a majority of the people, especially in developed and the elite in developing economies, relies on the Internet, either directly or indirectly, for most services. What is interesting is that this trend is not expected to slow down soon especially with ever increasing globalization[2]. Concomitant to this phenomenal growth of the Internet is the fact that it has occasioned a number of challenges most of which revolve around its universal and trans-territorial character allowing direct, instantaneous and multifaceted exchange of information among literally tens of millions of users over global computer networks. This trans-nationally dominant and free nature of the Internet was the conventional wisdom in the 1990s[3].

A number of legal principles have been tested in the courts as a result of this global reach of the Internet. In the Australian case of *Dow Jones & Company Inc. v Gutnick*[4] for example, the High Court of Australia asserted jurisdiction in proceedings relating to online defamation where the alleged defamatory material uploaded on the Internet in New Jersey, United States, was downloaded in Victoria by subscribers to an online business news service. The Court held that publication of the defamatory material had occurred in Victoria where the material was accessed by subscribers.

As already seen above, the Internet has revolutionized local and global communication given its trans-national and ubiquitous nature. A combination of these features and the anonymity embedded in its use has made the Internet an attractive tool for those with propensity to engage in unlawful acts. This presents significant challenges to governments and law enforcement agencies in regulating online activities[5]. It is feared that should current trends continue, the perception by users that the Internet is unsafe and therefore unsuitable for everyday use may become widespread and eventually lead to a loss of faith in "the system"[6]. It is believed that cybercrime, and other cyber-issues are the one area that could cause this type of loss of faith in the safety of the Internet.

II. CURRENT TYPES OF CYBERCRIME

Cybercrime, not unlike other forms of crime, is a multi-faceted and ever-changing problem. The conventional definition relates it to crime that involves a computer and a network. Ordinarily, the computer may be a platform for the commission of a crime or it may be the target. In its broader sense cybercrime boils down to criminal exploitation of the Internet. Attendant unlawful activities around this type of crime

*Secretary/CEO, Kenya Law Reform Commission, Kenya.

[1] See generally, Brian Fitzgerald et al, '*Internet and E-Commerce Law: Technology Law and Policy*' (Lawbook Co, Sydney, 2007).

[2] See generally Claude Barfield et al. (eds), *''Internet, Economic Growth and Globalization' Perspectives on the New Economy in Europe, Japan and the USA* (Springer-Verleg, Berlin 2003); and Jack Goldsmith and Tim Wu, *'Who Controls the Internet? Illusions of a Borderless World'* (Oxford University Press, Oxford, 2006) 79-81.

[3] See, e.g., John Perry Barlow, *'A declaration of the Independence of Cyberspace'* (1996) <http://homes.eff.org/~barlow/Declaration-Final.html>at 12 April 2008.

[4] (2002) 210 CLR 575; (2002) 194 ALR 433; (2002) HCA 56.

[5] See, e.g., Fitzgerald, above n 2,691-2.

[6] Michael Barrett, et al. "Combating Cybercrime: Principles, Policies, and Programs" April 2011 <www.paypal-media.com/assets/pdf/fact_sheet/... > 5 May 2015.

include: computer hacking, copyright infringement, identity theft, child pornography and child grooming[7].

In conversations on activities of government and non-state actors alike, one ordinarily comes across related variants of cybercrime such as cyberespionage, cyberwarfare and cyberterrorism. Cyberespionage refers to the process of hacking into computer systems in order to steal information, especially if the information is deemed to be of commercial value. A common example of this is 'industrial espionage' which occurs when unscrupulous companies spy on competitors and even on individuals[8].

Cyberterrorism on the other hand is evidenced by attacks against one or more parts of the Internet with the aim of precluding legitimate users from being able to use internet-based services, to instill fear that the integrity of services has been compromised, and most importantly to cause fear in the power of the group behind the attack[9]. It has been explained that the difference between cyberterrorism and cyberwarfare lies in three aspects: intention, scale, and actor. As such the intention in a full-scale cyberwar is to cripple the target (be it the economy, communications or essential services), or to create confusion prior to or during an actual attack. In these situations, direct control by the state or close collaboration of the state with these actors cannot be ruled out[10].

A number of cyberthreats have recently been identified. These comprise:

(a). Malicious Code: This includes any 'hardware, software or firmware' that is intentionally included or inserted in a system for a harmful purpose, commonly referred to as malware. Most common examples are computer viruses and other kinds of spyware (unauthorized programmes) installed to monitor a consumer's activities without consent.

(b). Network Attacks: These are basically actions taken to disrupt, deny, degrade or destroy information residing on a computer and computer networks. It may take the form of fabrication, interception, interruption and modification of information. One hears of terminologies like Denial of Service (Dos) and Distributed Denial of Service (DDos), among others.

(c). Network Abuse: These include fraudulent activities committed with the aid of a computer. SPAM (sending of unsolicited commercial mails from harvested email addresses) is a common example.

(d). Social Engineering: This occurs when people are manipulated into performing actions or divulging confidential information such as through e-mail phishing.

III. EFFECTS OF CYBERCRIME

Since the Internet allows digital anonymity, it is used by persons with ill intentions in ways that negatively affect the population both in the online and offline worlds. Crime such as identity theft is a common example. This occurs especially when one believes a request for personal information is coming from trusted and genuine sources such as banks or other financial institutions, only for the criminal to access the bank and credit accounts or open accounts and destroy the victim's credit rating.

Takeover of businesses by hackers to steal company information or use of company servers for nefarious purposes is another negative example. The high cost of piracy in monetary losses and its negative effects on the entertainment, music and software industries cannot be overemphasized. The effects of a single, successful cyberattack can have far-reaching implications including financial losses, theft of intellectual property, and loss of consumer confidence and trust. The overall monetary impact of cybercrime on society and government is estimated to be billions of shillings per year. In 2012, Deloitte Company noted that banks in East Africa alone lost about Kenya Shillings (Kshs) 4 billion to fraudsters who took advantage of weak security mechanisms[11].

[7] See, e.g., Fitzgerald, above n 2,953.

[8] See Barrett, above n 7.

[9] Ibid.

[10] Ibid.

[11] See Lilian Ochieng, 'Tough Law to Boost Fight Against Cybercrime' *Daily Nation Kenya*, 28 January 2014.

IV. STATE OF CYBERCRIME LAW IN KENYA

Kenya has for a long time lacked proper mechanisms to counter cybercrime. A cybercrime countermeasure is defined as an action, process, technology, device or system that serves to prevent or mitigate the effects of a cyberattack against a computer, server, network or associated device. A countermeasure can either be technical or regulatory; technical in the sense that computer and network users are advised to use internet protection such as strong, unique passwords to protect themselves from hackers while regulatory measures include legal frameworks that define and detail the conditions for prosecution of cybercrime.

In Kenya, the Kenya Information and Communications Act of 2009[12] establishes a body known as the National Computer Emergency Response Team (CERTS), whose mandate is to fight cybercrime in Kenya. Kenya has chaired the Cyber Security Taskforce of the East African Regulatory Postal and Telecommunication Organization (EARPTO) whose main objective is to facilitate the establishment of national CERTS in the East African region. In February 2012, Kenya entered into an agreement with a United Nations agency on the implementation of a national focal point for coordinating responses to cybersecurity incidents in the country.

The Kenyan government, through the Communications Authority[13] also signed an Administrative Agreement for the implementation of the Kenya National Computer Incident Response Team Coordination Centre, which would be the national trusted organ for advising and coordinating responses to cybersecurity incidences in Kenya, liaising with the local sector computer incident response teams, gathering and disseminating technical information on computer security incidents, carrying out research and analysis on computer security, thus facilitating the development of key public infrastructure and capacity building in information security.

The Kenyan government is working with the International Criminal Police Organization (INTERPOL) to combat cybercrime in Kenya. Consequently, Kenya is able to leverage on INTERPOL's technical guidance for combating cybercrime, including detection, forensic evidence collection, and investigation. An information technology crime investigation manual provides a technological law enforcement model to improve the efficiency of combating cybercrimes.

Kenya has also made several attempts in its laws to seek to curb cybercrime, the most distinct being the amendment to the Evidence Act[14] to allow the admissibility of digital evidence in court. However, this is not conclusive as the Interpretation and General Provisions Act[15] has not been amended and still requires the production of a physical document for purposes of adducing evidence in court. This means that the production of information and evidence generated, sent or stored in magnetic, optical or computer memory is still contentious. Another law covering this area is the Central Depositories Act[16] which provides stiff penalties for manipulation of electronic data.

V. CHALLENGES

The main challenge with the Kenyan legal regime is that The Kenya Information and Communication Act[17] mostly relates to electronic and mobile transactions and contains only few sections which deal with issues of cybercrime in the country. Moreover, the detailed procedural law provided for in the Convention on Cybercrime[18] is also lacking. One can therefore legitimately argue that this law was not enacted with cybercrime, as we currently know it, in mind. Again as already seen, there is apparent lack of uniformity in the diverse pieces of legislation amended ostensibly to deal with cybercrime. The other challenge relates

[12] Chapter 411A of the Laws of Kenya.

[13] Ibid.

[14] Chapter 80 of the Laws of Kenya.

[15] Chapter 2 of the Laws of Kenya.

[16] Act No 4 of 2000 (Laws of Kenya).

[17] Ibid.

[18] The *Convention on Cybercrime (The Budapest Convention on Cybercrime)*, opened for signature 23 November 2001, CET 185 (entered into force 1 July 2004).

to investigation and prosecution of cybercrimes. This is evidenced by limited understanding of information and technology issues and cybercrimes and its modus operandi by law enforcement officers who end up applying obsolete investigative techniques for sophisticated cybercrimes. Closely related to this challenge is the issue of processing of digital evidence in which Kenya lacks massively as there is no digital forensic laboratory for such kinds of crimes.

It is with the these realizations that in early 2014, the Office of the Director of Public Prosecution and the Kenya Law Reform Commission began the process of developing the Cyber Crime and Computer Related Crimes Bill, 2014[19] which seeks to equip law enforcement agencies with the necessary legal and forensic tools to tackle cybercrime, which is said to have cost the Kenyan economy nearly Kshs. 2 billion in 2013. The Director of Public Prosecutions has also established a special dedicated unit that will handle all cybercrime related cases in the country.

The draft bill is to address offences against confidentiality, integrity and availability of computer data and systems. This bill, if passed, will go down as the most effective cybersecurity law in Kenya as it makes provision on use of electronic evidence against the accused and at the same time focuses on police investigations and prosecutions. Evidence generated from a computer system will also be admissible in a court of law while prosecuting such a crime. The bill has introduced strict regulations that restrict internet usage and online protection of data such that a person is required to have a digital certificate to transact online. This will enable the authorities to know who is committing which crime online.

The bill gives courts within the country jurisdiction to try any Kenyan citizen who commits an offence anywhere in the world. Those found guilty of committing the offence on a ship or aircraft registered in Kenya, using a Kenyan domain name or outside the territory of Kenya will also be prosecuted in Kenyan courts. They will either be fined Kshs. 2 million, be imprisoned for three years or face both penalties.

The bill also proposes that a person, who causes a computer system to perform its functions, knowing that the access they intend to secure is unauthorized, commits an offence. It also proposes that a person who sells, lets to hire, distributes, publicly exhibits through a computer system, and puts into circulation, or for purposes of sale, hire, distribution, public exhibition or circulation, makes, produces or have in their possession any obscene book, pamphlet, paper, drawing, painting or any obscene object commits an offence.

Those using computers to threaten, abuse or use insulting words or behaviour, display, publish or distribute written or electronic material; or distribute, show or play a recording of visual images will be held accountable. The bill also proposes action against a person who uses a computer system including electronic communication to harass, intimidate or cause substantial emotional distress or anxiety to another person. These include communicating obscene, vulgar, profane, lewd, lascivious, or indecent language, pictures or images. Courts will also issue a warrant authorizing a police officer or lawful authority, to enter any premises to access, search and seize the thing or computer data.

All public or private corporations processing personal data will be expected to report any security breaches resulting in theft, loss or misuse of data to the police, and those who fail to do so will be committing an offence

VI. CONCLUSION

We are of the arguable view that, to date, no legislation has succeeded in totally eliminating crime from the globe and so is the case with cybercrime. Recent experiences show that Kenya's cybersecurity remains quite weak, exposing mobile phone subscribers and internet users to data interception and also making it difficult to prosecute cybercrime suspects. This follows the arrest of 37 Chinese citizens who were arrested in Runda Estate, Nairobi on December 2, 2014. They were allegedly found in possession of laptops, routers and mobile phones and were believed to be preparing to instigate serious crimes. The biggest challenge in prosecuting such crimes is lack of legal framework. Further, in April 2014, a Bangladeshi hacker was able

[19] The Draft Cybercrime and Computer Related Crimes Bill, 2014. For a detailed critique of the bill, see ARTICLE 19, Analysis of the Draft Cybercrime Law of Kenya, 2013 at <www.article19.org/.../Kenya-Cybercrime-Bill-129072014-BB.pdf> 5 May 2015.

to access a Kenyan domain belonging to major service providers such as Google, Microsoft, LinkedIn, HP and Dell. Millions of users on the networks were redirected to the hacker's site which showed the message that the sites had been hacked. This reveals the high level of exposure to cybercrime in the country and worldwide. Needless to say, cybercriminals require close cyber-expert surveillance since the anonymity associated with these crimes makes detection onerous.

Based on the foregoing analysis we propose the enactment of the Cyber Crime and Computer Related Crimes Bill 2014 as it contains comprehensive deterrence measures and a legal framework for prosecution of cybercrimes.

COMBATING CYBERCRIME IN THE PHILIPPINES

*Karla T. Cabel**

I. INTRODUCTION

On August 6, 1991, the World Wide Web (WWW) service, through the World Wide Web Project (WWW Project), made its debut to the public in the Internet. Englishman Tim Berners-Lee, the proponent of the WWW Project, envisioned that its debut would enable physicists from all over the world to conveniently share information, data, documentation and news with each other. Apparently, the public wanted to use the web for other areas and, thus, the first web message, "Collaborators welcome" of Berners-Lee, became a gateway, which allowed servers to share data on various areas of interest apart from physics.

It cannot be gainsaid that the vast majority is now enjoying the commercialization of the WWW in the 1990s. Today, the Internet has not only become a repository of information but also a tool in commerce, entertainment and social networking, both for the private sector and the government. In fact, transactions are now borderless. Credit is given to globalization, technology and the dynamic and young people of the generation.

However, the pairing of high technology and globalization results in crime in as much as borderless transactions result in borderless crimes. Today, many traditional crimes are now being committed using the computer and Internet. As correctly observed by then Federal Bureau of Investigation Director Robert Mueller, "crimes have migrated online, including various frauds, identity theft, copyright infringement, child pornography and child exploitation."[1] In one case, a teenager defrauded people of an estimated $5,000 through an on-line auction scam by advertising allegedly high-end computer equipment for sale in the Internet when, in truth, he was actually selling equipment of lesser value to unsuspecting buyers.[2]

In another case, a blogger was convicted for libel when he vented his frustration with his lawyer by calling the latter a "drug bribery mule", on his website.[3] Meanwhile, the Australian High Court allowed criminal proceedings to be held in Australia even if the servers of the article, which is the subject of the complaint, are located in New Jersey. The court ruled that the "claim could be brought only if a person had a reputation in the place where the material was published."[4]

II. CHARACTERISTICS OF CYBERCRIME AROUND THE WORLD

A. Types of Cybercrime and Modus Operandi

According to the Australian Institute of Criminology, there are nine (9) types of cybercrimes[5], *viz*:

1. Theft of Telecommunications Services

This occurs when offenders gain access to an organization's telephone switchboard (PBX) or dial-in/dial-out circuits, by impersonating a technician, fraudulently obtaining an employee's access code or by

*Prosecutor, Department of Justice, Padre Faura, Manila, Philippines.

[1] Targeting Cybercrime, The Philippine Star, <http://www.philstar.com/networks/184074/targeting-cybercrime> accessed February 19, 2015.

[2] Sullivan, Confessions of a Scam Artist, MSNBC, September 2002.

[3] *Milum vs. Banks*, Court of Appeals, Georgia, Case No. A06A2394, March 5, 2007.

[4] *Gutnick v Dow Jones & Co Inc.* [2001] VSC 305 (28 August 2001)', <http://www.austlii.edu.au/au/cases/vic/VSC/2001/305.html>.

[5] *9 Types of Cyber Crime*, Australian Institute of Criminology, Crime in the Digital Age by Peter Grabosky and Russell Smith, Sydney: Federation Press, 1998 (co-published with the Australian Institute of Criminology), <http://www.crime.hku.hk/cybercrime.htm> accessed February 19, 2015.

using available internet software, and use the same to make their own calls or sell call time to third parties (Gold 1999). Other forms may include "calling card details and on-selling calls charged to the calling card account, counterfeiting or unlawfully reprogramming stored value telephone cards.

2. Communications in Furtherance of Criminal Conspiracies

This involves organized criminal activities enhanced or facilitated by technology, such as weapons smuggling, money laundering, drug trafficking, gambling, prostitution and child pornography (Grant, David and Grabosky 1997).

Criminal networks have been discovered to extend transnationally, work with a significant degree of coordination and use sophisticated means of concealment. An example would be the police investigation codenamed "Operation Cathedral", which involved "Wonderland Club", an international network with 14-member nations from Europe, North America to Australia, where members can access the group and its encrypted content via password. The operation resulted to 100 arrests worldwide and seizure of over 100,000 images in September 1998.

3. Telecommunications Piracy

This involves the unauthorized reproduction of copyrighted materials for free distribution, personal use or for sale at a lower price.

Owners of the copyrighted materials are estimated to have incurred losses between $15 - $17 billion due to copyright infringement (United States, Information Infrastructure Task Force 1995, 131). The Software Publishers Association claims that it lost $7.4 billion worth of software due to piracy in 1993, of which $2 billion were stolen from the Internet (Meyer and Underwood 1994). Ryan (1998) states that American industry lost more than $10 billion in 1996, from which $1.8 billion is the estimated loss in the film industry, $1.2 billion in music, $690 million in book publishing and $3.8 billion in business application software.

4. Dissemination of Offensive Materials

This includes dissemination of objectionable materials in the Internet such as racist propaganda, sexually explicit materials and instructions for making incendiary and explosive devices, use of telecommunications systems for threatening or intrusive communications, harassing, "cyber-stalking" and other means where persistent messages are sent to unwilling recipients as well as the use of computer networks in furtherance of extortion. On June 2, 1996, the Sunday Times in England cited 4 incidents between 1993 and 1995 where senior executives of financial institutions paid £42.5 million to extortionists they believed could crash their computer systems (Denning 1999, 233-4).

In one case, a man stole nude photographs of his ex-girlfriend and new boyfriend, posting them on the Internet, along with her name, address and telephone number and maintaining records about the woman's movements and collating information about her family (Spice and Sink 1999).

A rejected suitor, using the name of the woman he courted, posted invitations on the Internet that she had fantasies of rape and gang rape, and gave out her personal information, address, phone number, her appearance and how to bypass her home security system, to which men replied and appeared at her home. Although the lady was not physically assaulted, she would not leave her home or answer the phone. She eventually lost her job (Miller 1999; Miller and Maharaj 1999).

A student in California bought information about a woman in the Internet using a professor's credit card and then sent death threats and graphic sexual descriptions to 5 female students in 1998, in response to perceived teasing about his appearance (Associated Press 1999a).

5. Electronic Money Laundering and Tax Evasion

This involves concealing and moving proceeds of crime through electronic funds transfers (money laundering) or concealing legitimately derived income from the government's taxing authorities (tax evasion) using technologies of electronic commerce.

6. Electronic Vandalism, Terrorism and Extortion

Electronic intrusion such as hacking official websites of the government or private companies, i.e. attempts to disrupt the computer systems of the Sri Lankan Government (Associated Press 1998) and North Atlantic Treaty Organization during the 1999 Belgrade Bombing (BBC 1999); German hackers who compromised an internet service provider in South Florida and demanded the delivery of $30,000 to a mail drop in Germany (Bauer 1998); and credit card details of a music retailer in North America having been obtained by an extortionist in Eastern Europe who published the details of the former on the Internet when he refused to comply with latter's demands (Markoff 2000).

7. Sales and Investment Fraud

The use of cyberspace for misinformation by directly accessing victims worldwide. This includes classic pyramiding schemes and bogus investment opportunities and investment solicitations (Cella and Stark 1997, 822).

8. Illegal Interception of Telecommunications

This involves electronic eavesdropping, such as surveillance of an unfaithful spouse, telecommunications interception and industrial espionage, by intercepting electromagnetic signals from computers. An example is the case of an American hacker, Kevin Poulsen, who accessed law enforcement and national security wiretap data (Littman 1997).

9. Electronic Funds Transfer Fraud

This involves the electronic and physical interception of valid credit card numbers and counterfeiting of digital information stored on a card.

In 1994, Russian hacker Vladimir Levin, was able to access Citibank's central wire transfer department and transferred money from large corporate accounts to the accounts of his accomplices in the United States, Finland, Germany, Netherlands and Israel. A corporate owner in Argentina notified the bank, which resulted in the arrest of his accomplices in San Francisco and Rotterdam. Levin was later arrested during a visit to the United States (Denning 1999,55).

B. Damages Caused by Cybercrime

Cyber-attacks have become a regular occurrence since the ubiquity of the Web. Cybercrime espionage and pilfering of personal information is believed to have affected more than 800 people during 2013. Financial losses from cyber-theft can cause as much as 150,000 European jobs.

Sometime in August 2014, there was a mass breach of privacy when about 200 images of various celebrities were posted on the image-sharing site "4chan". Most of them were intimate photos of women. The images, which were allegedly hacked from the iCloud of Apple, spread through Twitter and Reddit and other various social media sites.[6]

Still, in November 2014, a group called the "Guardians of Peace", allegedly acting in retaliation against Sony Pictures Entertainment for the release of the movie "The Interview" (a fictional story about a CIA plot to assassinate Kim Jong-un, the North Korean dictator), hacked thousands of Sony's private documents and emails. In December 2014, "Guardians of Peace" threatened cinemas with terrorist violence if the film were shown and, thus, caused several movie theaters' refusal to run it. The US Director of National Intelligence James Clapper contends that it was the North Korean General Bureau of Reconnaissance that supervised the hacking attack and that it may have caused Sony "potentially hundreds of millions of dollars in damage".[7] The attack rendered thousands of Sony computers inoperable such that the company had to take the entire network offline. Despite these assertions, experts state that there is no evidence that North Korea was behind the attack. Sony's CEO Kaz Hirai remarked that Sony was a victim of one of the most vicious and malicious cyberattacks in recent history.

[6] *Celebrity 4Chan Shock Naked Picture Scandal: Full List of Star Victims Preyed Upon By Hackers*, <http://www.mirror.co.uk/3am/celebrity-news/celebrity-4chan-shock-naked-picture-4395155> accessed February 19, 2015.

[7] *Sony Pictures Hack: US Intelligence Chief Says North Korea Cyberattack Was 'Most Serious' Ever Against US Interest*, <http://www.independent.co.uk/news/world/americas/us-intelligence-chief-sony-hack-was-most-serious-attack-against-us-interests-99> accessed February 19, 2015.

On December 22, 2014, a cyberattack against a German steel mill resulted to massive damage. According to the report of the German Federal Office for Information Security (BSI), the attackers used a "spear phishing" campaign aimed at particular individuals of the company to trick people into opening booby trapped emails to steal logins to access the mill's control systems. This led to failure of the plant's blast furnace to shut down normally. The unscheduled shutdown caused immense physical damage to the steel mill.[8]

More recently, on February 4, 2015, a video was aired showing Jordanian pilot Lt. Muath al-Kaseasbeh being burned alive by the Islamic State of Iraq and Syria (ISIS). The images of the killing triggered global condemnation and Jordan's promises of immediate retaliation[9]. And yet again, on February 15, 2015, ISIS released a new video showing the beheading of 21 Coptic Egyptian Christians on a Libyan beach.[10]

In 2014, reports state that the global economy is losing $445 billion annually.[11] However, recent estimates reveal that the cost of cybercrime to businesses worldwide range from $445 billion (£291 billion) to $2 trillion (£1.3 billion) a year. The cost of cybercrime will continually increase since transactions are now moving online as more companies and consumers connect to the Internet worldwide. Intellectual property theft losses will also increase because acquiring countries continually improve their abilities to manufacture competing goods.

These are but few examples of cybersecurity-related damages and cyber-sabotage, which terrorists and/or hostile elements could mount. Indubitably, cybercrime is becoming more pervasive through the years. Measures to secure cyberspace will be fraught with challenges since the Internet was designed to promote connectivity and not security. Still, governments should come up with effective ways to collect and publish cybercrime-related data to enable its people to make better choices on Web-related risks and policies.

III. THE CYBERCRIME PREVENTION ACT OF 2012 OF THE PHILIPPINES

In reply to the challenges of cybercrime, the Philippines enacted its first law regulating the WWW on June 14, 2000, Republic Act No. 8792 (Philippine Electronic Commerce Act of 2000). This was done after a criminal complaint, which was filed against the suspected creator of the email Trojan called "ILOVEYOU", was dismissed due to then absence of concrete laws regulating the Web in the Philippines.

On September 12, 2012, Republic Act No. 10175 (The Cybercrime Prevention Act of 2012) was signed into law. However, the law became effective only after the Supreme Court of the Philippines upheld the validity of its salient parts in its Decision dated February 18, 2014.[12]

IV. THE INVESTIGATION, PROSECUTION AND ADJUDICATION OF CYBERCRIME

A. Initial Information Gathering

1. Cyberpatrol

The Cybercrime Division of the National Bureau of Investigation (NBI) and the Anti-Cybercrime Group of the Philippine National Police (PNP) are the law enforcement agencies (LEA) responsible for the investigation and prevention of cybercrime in the Philippines. They are also required, under the law, to submit regular reports, including pre-operation, post-operation and investigation results and other documents,

[8] *Hack Attack Causes 'Massive Damage at Steel Works*, BBC News, December 22, 2014 <http://www.bbc.com/news/technology-30575104> accessed February 19, 2015.

[9] *Fox News Airs Images of Burning Jordanian Pilot*, Huffpost Media, February 4, 2015, <http://www.huffingtonpost.com/2015/02/04/fox-news-burning-isis-hostage-jordanian-pilot-images-pictures_n_6612446.html> accessed February 19, 2015.

[10] *ISIS Posts Video of Purported Mass Beheading*, CNN International Edition, February 15, 2015 <http://edition.cnn.com/videos/world/2015/02/15/isis-video-purports-21-coptic-christian-hostages-beheaded.cnn> accessed February 19, 2015.

[11] *Cybercrime Costs Global Economy $445 BN Annually*, Rhiannon Williams, June 9, 2014, <http://www.telegraph.co.uk/technology/internet-security/10886640/Cyber-crime-costs-global-economy-445-bn-annually.html> accessed February 19, 2015.

[12] *Disini, et. al. vs. The Secretary of Justice, et. al.* GR Nos. 203335, 203299, 203306, 203359, 203378, 203391, 203407, 203440, 203453, 203454, 203469, 203501, 203509, 203515, 203518, February 18, 2014.

which may be required by the Department of Justice – Office of Cybercrime (DOJ-OOC) for review and monitoring.[13]

2. Reporting System

The Department of Justice of Justice – Office of Cybercrime (DOJ-OOC) is the central authority in the monitoring of all matters relating to cybercrime. Its functions also include receiving regular reports from the LEA.[14]

B. Tracing and Identifying Criminals, Preserving and Collecting Evidence

1. Tracing and Identifying by IP Address and other Measures

The first step in prosecuting cybercrime cases is for the responsible LEA to identify who the criminal is by determining his/her Internet Protocol Address (IP Address)[15]. The challenge online is that there are innumerable measures to hide one's identity, such as the use of services that will mask a user's IP Address by routing traffic through various servers.

However, diligence pays in tracking down cybercriminals. It has been observed in several cases that those who engage in cyber-stalking or cyber-fraud, to name a few, are not technically savvy and may leave clues as to their identity within the content of the data. It has been further observed that even experts may inadvertently leave clues due to their complacency or sheer arrogance.

Ordinarily, IP Address can be extracted through the header information of emails and system logs. Once the IP Address has been identified, the said IP Address is then subjected to a WHOIS search, a query and response protocol that is widely used for querying databases that store the registered users or assignees of an internet resource[16], to verify which Internet Service Provider (ISP)[17] it belongs to. Examples of WHOIS lookup capable websites are "www.Checkdomain.com" and "www.apnic.net".

When the ISP is identified, a Preservation Order is then sent to the ISP requiring it to preserve the integrity and content of the data in their custody for a minimum period of six (6) months from the date of receipt of the said order[18]. The law provides that the Service Provider shall keep confidential the order and its compliance.

2. Real-Time Collection of Traffic Data and Interception of Content Data

It is recommended that the LEA conduct a thorough investigation before executing a search warrant of the scene of computer-related crime to avoid delays since they will know in advance what to expect at the crime scene and will be able to determine whether there is a need for experts for purposes of collecting data.

The LEA may conduct either technical surveillance or physical surveillance in their investigation. Technical surveillance, if applicable, is done by visiting the website concerned with the intention of downloading resource materials therefrom and establishing communication with the subject through email. On the other hand, physical surveillance entails verifying the existence of the addresses provided by the ISP by going to the indicated address and comparing the results to the information received.

3. Fair and Timely Search, Seizure and Preservation of Digital Evidence

Using the resource materials and valuable information obtained from the surveillance, the LEA will then secure a search warrant from the court. Thereafter, pursuant to the said warrant, it shall order the ISP to disclose or submit the subscriber's information, traffic data or relevant data in its possession or control within seventy-two (72) hours.[19]

[13] Sec. 11, Ibid.
[14] Sec. 23, Ibid.
[15] IP Address – series of numbers assigned by an Internet Service Provider to an internet user when it connects to the Internet. Anchor of all crimes committed via Internet.
[16] <En.wikipedia.org/wiki/Whois> accessed February 20, 2015.
[17] Internet Service Provider – provides internet service to internet users.
[18] Sec. 13, Republic Act No. 10175.
[19] Ibid.

It is recommended that the execution of the warrant be documented either through writing, sketching, photographs and/or video. Situational awareness is paramount. Thus, it is crucial to always secure and take control of the scene bearing in mind the team's safety. As soon as the area has been secured, the forensic investigator may now run the incident response (IR) tools and save volatile data. The LEA should not access computer files in the search area. If the computer is off, it should be left off. If it is on, they should refrain from searching the computer. Instead, photograph the screen, if something is displayed on the monitor, and consult with the on-site forensic investigator.

When executing the search warrant, the LEA should keep individuals, especially the suspect, away from computer equipment to avoid corruption of the data. However, if the computer appears to be destroying the evidence, they should immediately shut it down by pulling the power cord.

The LEA should secure the seized evidence by properly bagging[20] and tagging[21] them and placing them in non-magnetic containers to be examined by a certified forensic media analyst. The LEA should properly transport electronic evidence obtained from the crime scene. The computer evidence should not be exposed to heat and radio transmission. Radio transmitters can damage the hard drive and destroy the evidence. Meanwhile, the evidence should be stored in an area inaccessible to unauthorized persons. Cool and dry storage facilities away from generators and magnets are ideal.

4. Technical Analysis of Digital Data

Evidence should be evaluated with the assistance of experts on digital forensics[22]. This is because computer evidence require knowledge in a wide array of programming systems, such as d-base III, Lotus 1-2-3 and other word processing languages, which are not known even to the best trained investigators. Since digital evidence can be easily altered, its analysis should be done by experts to preserve its integrity and authenticity. Digital forensics determines the cause of the cybercrime, the manner in which it was committed, leads on the cybercriminal and existence of contraband by analyzing not only digital data but also its relation to the pieces of documentary evidence recovered from the area of search.

C. Prosecution

1. Appropriate Evaluation of Digital Evidence

Although digital evidence is accorded evidentiary value as other forms of evidence, i.e. object, documentary, testimonial, there is always hesitation in presenting them in court. This is attributed to the complexity of digital evidence, lack of technical know-how of both the bench and bar and improper collection of digital evidence. But what makes digital evidence the least favorite among other forms of evidence is that it is "extremely vulnerable to inadvertent or intentional modification or destruction".[23]

A simple misstep in the collection of digital evidence can affect the integrity of the data content. Improper handling and storage of digital evidence can easily corrupt it, and evidence haphazardly gathered by untrained investigators may be excluded by the court for incompetence.

Apropos, digital evidence should be properly evaluated before it is presented in court.

To avert issues on the integrity and authenticity of digital evidence, it is recommended that LEA apply for search warrants when seizing digital evidence.[24] This will ensure that the evidence is properly documented, gathered, identified, examined and preserved.

In drafting the affidavit application of the warrant, the LEA will indicate therein the facts established through an Internet Protocol (IP) Address, subscriber account, or mobile phone number, call logs for a specific period or duration, describe with particularity the data or information to be disclosed and the

[20] Bagging – protects against contamination and tampering.

[21] Tagging – provides means of associating the attached and bagged evidence with a particular date, time, location, place event and seizing agent.

[22] Digital Forensics – refers to the application of investigative and analytical techniques that conform to evidentiary standards used in or appropriate for a court of law of other legal context.

[23] McCullagh, *Electronic Evidence Anchors Porn Case*, Tech News CNET.com, August 29, 2002.

[24] Manual of Guidelines in Investigating Cybercrimes.

specific violation of the law.[25]

In the recent landmark case of *Riley vs. California*, the 4th Appellate District, Division One of California, ruled that warrantless police searches of the contents of an arrestees' cell phones is not allowed. It opined that cellphones are tiny computers with highly private data and accessing them is different from going through someone's pockets or purse.[26]

Note, however, that in *Warshak vs. United States of America*[27], the Sixth US Circuit Court of Appeals proscribed investigators from conducting email searches in a fraud case filed against an individual ruling that e-mail users maintain a "reasonable expectation of privacy in the content of their emails". It held that although a third party has access to email, like an internet service provider, this does not mean that a subpoena can compel the said provider to defeat the accused's privacy by opening the latter's emails and presenting them to the investigators.[28]

As regards the evaluation of digital documents, such as computer print-outs and e-mails, the law provides that they are considered admissible provided they comply with rules of admissibility under the Rules and that they are properly authenticated.[29] Further, electronic documents are authenticated by evidence showing that they have been digitally signed by the person purported to have signed the same, evidence that appropriate security procedures or devices for authentication of electronic evidence were applied and by evidence showing its integrity and reliability to the satisfaction of the judge.[30] In one case, the Supreme Court ruled that the computer print-outs which were submitted in evidence were unauthenticated, unreliable and, thus, found them insufficient to establish the allegations of absenteeism and tardiness.[31]

It is also necessary that the chain of custody of digital evidence is observed when evaluating the said evidence. It is always the burden of the prosecution to convince the court that the digital evidence being offered has not been modified or replicated. Thus, any change in the chain of custody must be properly documented. Otherwise, the evidence may not be presented at a later date or be discarded by the court for lack of authenticity and integrity.

2. Identifying Criminal Acts and Proper Selection of Cybercrime Charges

Republic Act No. 10175 enumerates and defines cybercrime offences. According to the said law, punishable offences are as follows: (i) those offences against the confidentiality, integrity and availability of computer data and systems, *viz*: illegal access[32], illegal interception[33], data interference[34], system interference[35], misuse of devices[36] and cybersquatting[37]; (ii) computer-related offences, *viz*: computer-related forgery[38], computer-related fraud[39], computer-related identity theft[40]; (iii) content-related offences, *viz*: cybersex[41], child pornography[42] and libel[43] (iv) other cybercrimes, *viz*: aiding, abetting and attempting to commit punishable acts enumerated under the said law and (v) crimes committed under the Revised Penal Code and Special Laws, if committed by, through and with the use of information technology.

Apart from being charged for violation of Republic Act No. 10175, the offender may also be charged for

[25] Section 4, Republic Act No. 10175.
[26] *Riley vs. California*, Case No. 13-132, June 25n, 2014.
[27] *Warshak vs. US*, Case No. 06-4092, June 18, 2007.
[28] *Warshak vs. US*, supra.
[29] Section 2, Rules on Electronic Evidence.
[30] Section 2, Rule 5, Ibid.
[31] *Asuncion vs. National Labor Relations Commission, et. al.*, G.R. No. 129329, July 31 2001.
[32] Illegal Access – the access to the whole or any part of computer system without right (Sec.4 par.a[1], R.A. No. 10175.
[33] Illegal Interception – the interception made by technical means without right of any non-public transmission of computer date to, from a computer system carrying such computer data (Sec. 4, par.a[2], Ibid).
[34] Data Interference – intentional or reckless alteration, damaging, deletion or deterioration of computer data, electronic document, or electronic data message, without right, including the introduction or transmission of viruses (Sec.4, par.a[3], Ibid).
[35] System Interference – intentional alteration or reckless hindering or interference with the functioning of a computer or computer network by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data or program, electronic document, or electronic data message, without right or authority, including the introduction or transmission of viruses (Sec.4, par.a[4], Ibid).
[36] (Sec.4, par.a[5], Ibid).

violating other related laws, such as Special Protection of Children Against Child Abuse, Exploitation and Discrimination (Republic Act No. 7610), as amended; Terrorism Financing Prevention and Suppression Act of 2012 (Republic Act No. 10168); Electronic Commerce Act (Republic Act No. 8792); Anti-Money Laundering Act 2001 (Republic Act No. 9160, as amended by R.A. 9194); Comprehensive Dangerous Drugs Act of 2002 (Republic Act No. 9165); Anti-Trafficking in Persons Act of 2003 (Republic Act No. 9208, as amended by Republic Act No. 10364); Anti-Photo and Voyeurism Act of 2009 (Republic Act No. 9995); Anti-Child Pornography Act of 2009 (Republic Act No.9775), E-Commerce Act of 2000 (Republic Act No. 8792); Access Device Regulation Act of 1998 (Republic Act No. 8484); Intellectual Property Code of the Philippines (Republic Act No. 8293) and for other common crimes under the Revised Penal Code of the Philippines.

V. CAPACITY BUILDING

Ill-equipped and ill-trained investigators in the field of cybercrime are anathema to the successful prosecution of cybercrime offences, not only in the Philippines, but worldwide. It is predicted that cybercrime will treble over the next three (3) years and yet the personnel in the Philippines involved in cybercrime are not prepared to deal with cyber-threats.

In November 2014, a group identified as "BloodSec International", defaced websites of the bills payment center Expresspay, the government's Technical Education and Skills Development-Calabarzon and the Philippine Society of Nephrology after attacking Globe Telecom's website.[44]

Still in November 2014, a group identified as "Anonymous Philippines" hacked 38 government websites posting a message calling Filipinos to join a protest against corruption.[45] In January 2015, various government websites were hacked again by Anonymous Philippines calling for justice for the 44 slain policemen of the Special Action Force of the Philippine National Police.[46]

To address this issue of readiness, from November 24-28, 2014, the OOC, in partnership with the Council of Europe (COE) and European Union (EU), conducted a Judicial and Law Enforcement Training Workshop on Cybercrime. The workshop integrated the tasks of the OOC in line with the COE EU Global Action against Cybercrime (GLACY) project. The training was attended by judges and law enforcers who are handling electronic evidence.

In February 2014, the OOC conducted the second phase of the Basic Cybercrime Ethical Hacking

[37] Cybersquatting – acquisition of domain name over the internet in bad faith to profit, mislead, destroy reputation and deprive others from registering the same.

[38] Computer-related forgery – input, alteration or deletion of computer data without right resulting to inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible or the act of knowingly using computer data which is the product of computer-related forgery as defined herein, for the purpose of perpetrating a fraudulent or dishonest design.

[39] Computer-related fraud – the unauthorized input, alteration or deletion of computer data or program or interference in the functioning of a computer system, causing damage thereby with fraudulent intent: Provided, that if no damage has yet been caused, the penalty imposable shall be one (1) degree lower.

[40] Computer-related identity theft – intentional acquisition, use, misuse, transfer, possession, alteration or deletion of identifying information belonging to another, whether natural or juridical, without right: Provided, that if no damage has yet been caused, the penalty impossible shall be one (1) degree lower.

[41] Cybersex – willful engagement, maintenance, control or operation, directly or indirectly, of any lascivious exhibition of sexual organs or sexual activity, with the aid of a computer system, for favor or consideration.

[42] Child-pornography- unlawful or prohibited acts defined and punishable by Republic Act No. 9775, committed through a computer system: provided, that the penalty to be imposed shall be one (1) degree higher.

[43] Libel – unlawful or prohibited acts of libel as defined in Article 355 of the Revised Penal Code, as amended, committed through a computer system or any other similar means which may be devised in the future.

[44] After Globe, More PH Websites Hacked, inquirer.net, <technology.inquirer.net/39602/after-globe-more-ph-websites-hacked> accessed February 21, 2015.

[45] *Antipork Hackers Hit 38 Government Websites*, <technology.inquirer.net/31145/antipork-hackers-hit-38-govt-website> accessed February 21, 2015.

[46] *Hackers Attack Government Sites, Call For Justice for Slain SAF Men, Nestor Corrales*, Inquirer.net, <technology.inquirer.net/40558/hackers-attack-govt-sites-call-for-justice-for-slain-saf-men> accessed February 21, 2015.

Training of law enforcers. This was graced by the operatives from the National Bureau of Investigation-Cybercrime Division (NBI-CCD) and the Philippine National Police-Anti-Cybercrime Group (PNP-ACG).

Since digital forensics in cyber-related offences is a complex subject, training programmes are not only given to law enforcers but also to prosecutors, state counsels and public attorneys in the Philippines. The coverage of the training includes procedures on cybercrime investigations, cyber-incident response and digital forensics.

The OOC will also launch the National Computer Forensics Training Program, a consolidated training for all law enforcers in computer forensics and provide them with structured procedures and guidelines consistent with international best practices.

Another challenge in cybercrime is interstate coordination. Rising incidents of cybercrime show that it is a global phenomenon where a cybercriminal stationed in one state executes his attacks in another unsuspecting state.

Thus, in January 2014, the OOC started formulating the Global Action on Cybercrime (GLACY) project country report and work plan. This is in partnership with the Council of Europe (COE). This project aims to enable criminal justice authorities to engage in international cooperation on cybercrime and electronic evidence on the basis of the Budapest Convention.

The OOC has also been coordinating with the United States Homeland Security Investigations (USHSI) Manila Attaché in the investigation of crimes, such as child pornography, with the use of the Internet. The coordination led to a successful operation and arrest of a subject in contact with an American sex predator in the United States sometime in February 2014.

Considering that combating child pornography is a priority of the OCC, the OOC is developing a centralized "flat file" database of child pornography collated from investigations and intelligence gathering. The database will be disseminated to all ISPs to serve as a reference for "filtering and blocking". The project is in collaboration with the International Police's International Child Sexual Exploitation (INTERPOL ICSE). INTERPOL will conduct training in the ICSE in April 2015.

VI. CONCLUSION

The growth of cybercrime is alarming. Recent surveys show that with advancements in technology and anonymity in the Internet, cybercrime will increase in severity and in number over the years. Be that as it may, cybercrime is a threat to all sectors of society worldwide. Private business entities such as banks, infrastructure, software companies, copyrighted materials and government offices are not spared from cyber-threats. A cybercriminal stationed in one country can commit a crime in another state with impunity.

Jurisdiction in cybercrime becomes a real issue especially when the perpetrator hides behind the veil of a country with unregulated cyber-activities. In this regard, the principle of sovereignty, which dictates that a law of one country cannot be imposed upon anther, becomes a bane to cybercrime prosecution. Crime is borderless but the enforcers are restricted by the borders of sovereignty.

With this realization, more and more countries are now adopting an inter-country cooperation approach against cybercrime. Inter-state treaties harmonize laws in signatory countries and establish systems of mutual cooperation.

Although some object to the "seeming" interference of foreign states on one's territory, the same is a small price to pay compared to the magnitude of damages and terror the cybercriminals can cause if they are allowed unabated access to the Internet.

PROSECUTING COMPUTER-RELATED CRIMES IN THAILAND

*Thongchai Itthinitikul**

I. THE STATE OF CYBERCRIME IN THAILAND

Currently, the Ministry of Information and Communication Technology (MICT) is implementing the digital economy policy declared by the Thai government as a policy statement to the parliament last year (2014). The MICT has played a key role to follow up the Thailand Information and Communication Technology (ICT) Policy Framework (2011-2020).[1] The framework comprises five strategic areas, namely e-Government, e-Industry, e-Commerce, e-Education and e-Society, that aim to enhance the economy and life quality of Thai people and guide Thailand towards a knowledge-based economy and society. This mission has mostly been assigned to the Electronic Transactions Development Agency (ETDA)[2] which is an agency (public organization) under MICT. ETDA serves as the core agency to develop, promote and support electronic transactions to ensure that they are reliable and provide equal opportunities to all. Although this development has brought great benefits and convenience to all Thai people and the country as a whole, it has also produced computer-related crimes which cause severe damage.

To mitigate and handle the aggressive growth of cybercrime, the Thailand Computer Emergency Response Team/Coordination Center, or ThaiCERT,[3] was transferred to ETDA from the National Electronics and Computer Technology Center (NECTEC) under the National Science and Technology Development Agency in 2011. The mission of ThaiCERT emphasizes collaboration with network agencies and concerned entities to cope with known ICT security threats. Furthermore, ThaiCERT has been assigned another proactive role in human resources development to enhance the agency's risk management capacity on cybercrime threats. Supported by ThaiCERT, ETDA's mission to build trust in electronic transactions has therefore been considerably strengthened. However, cybercrime issues in Thailand are still increasing and are becoming more aggressive as seen from the statistics of incidents reported to ThaiCERT from July 2011 till 2015 as follows.

*Divisional Public Prosecutor, Executive Director's Office of Criminal Litigation 10, Office of the Attorney General, Thailand.

[1] Available at <http://www.mict.go.th/assets/portals/10/files/e-Publication/Executive%20Summary%20ICT 2020.pdf>.

[2] Available at <http://www.etda.or.th/etda_website/content/background-and-mission.html>.

[3] Available at <http://www.etda.or.th/etda_website/eng/content/background-of-thaicert.html>.

Statistics of Incidents Reported to ThaiCERT[4]
Table 1: Statistics second half of 2011

Incident Type / Month	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec	Sum
Abusive content							12	8	6	7	39	5	**77**
Availability							1	2	2	0	1	0	**6**
Fraud							44	38	56	69	66	36	**309**
Information gathering							28	13	18	14	12	8	**93**
Information security							0	0	0	0	0	0	**0**
Intrusion Attempts							9	20	19	19	16	11	**94**
Intrusion							0	0	0	0	0	0	**0**
Malicious code							6	10	14	7	18	8	**63**
Other							0	0	0	1	0	3	**4**
Sum							**100**	**91**	**115**	**117**	**152**	**71**	**646**

Since operating under ETDA for the first six months (1 July to 31 December 2011), ThaiCERT received a total of 646 incident reports which can be categorized into nine incident classes. About 47.8% of the reports are related to fraud concerning phishing at domestic and international financial institutions. This kind of cybercrime directly impacts persons using electronic payment channels. The second most frequently received reports relate to attempts to attack and penetrate systems. In this incident class, 14.6% were intrusion attempts and 14.4% were information gathering incidents. Next were abusive content incidents identified as spam mail reaching 11.9%. The last were malicious code incidents, accounting for 9.8% of the reported attacks.

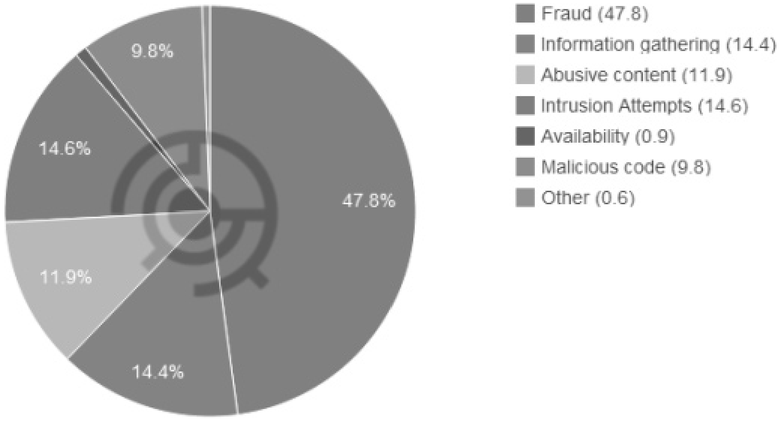


Figure 1: ICT Incidents between 1 July and 31 December 2011 by Incident Class
Statistics of Incidents Reported to ThaiCERT for the last two years 2013 and 2014

[4] Available at <https://www.thaicert.or.th/statistics/statistics-en2011.html>.

Table 2: Statistics 2013

Incident Type / Month	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec	Sum
Abusive content	1	2	3	1	1	2	0	0	0	1	2	0	**13**
Availability	1	0	0	0	0	0	0	8	0	1	0	0	**10**
Fraud	36	48	49	56	78	56	110	53	53	54	59	42	**694**
Information gathering	3	0	0	0	0	2	0	0	0	3	0	0	**8**
Information security	0	0	0	0	0	0	0	0	0	0	0	0	**0**
Intrusion Attempts	56	23	17	23	16	11	24	16	24	46	24	36	**316**
Intrusion	6	3	50	61	115	94	67	63	89	46	27	10	**632**
Malicious code	1	4	6	4	3	11	9	7	5	6	5	12	**73**
Other	0	0	0	0	0	0	0	0	0	0	0	0	**0**
Sum	**104**	**80**	**125**	**145**	**213**	**176**	**210**	**147**	**171**	**157**	**117**	**100**	**1745**

Table 3: Statistics 2014

Incident Type / Month	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec	Sum
Abusive content	1	1	0	0	0	0	3	1	1	1	0	0	**8**
Availability	0	0	2	2	0	0	1	3	0	0	0	0	**8**
Fraud	59	68	69	72	145	85	94	66	98	88	101	65	**1010**
Information gathering	1	2	6	8	7	0	1	1	3	0	0	0	**29**
Information security	0	1	0	0	0	2	0	0	1	0	0	0	**4**
Intrusion Attempts	39	28	32	51	43	30	42	40	30	46	48	74	**503**
Intrusion	9	150	77	33	55	50	69	47	86	32	35	68	**711**
Malicious code	3	7	129	125	102	226	304	161	263	98	132	185	**1735**
Other	0	0	0	0	0	0	0	0	0	0	0	0	**0**
Sum	**112**	**257**	**315**	**291**	**352**	**393**	**514**	**319**	**482**	**265**	**316**	**392**	**4008**

Compared to the figures in Table 1, the cybercrime incident reports in 2013 are similar in that the majority is still fraud followed by intrusion and intrusion attempts, respectively. Significantly, in 2014 the number of incident reports related to malicious code outnumbered the figures of the top three incidents reported in 2011 and 2013, and the total number of all attacks reported in 2014 is more than twofold compared to that of 2011 and 2013.

It could be concluded that cybercrime threats in Thailand are still increasing significantly even though both government and the private sector are aware of them and try to mitigate and handle this state of cybercrime. This trend is possibly attributed to the fact that a large number of computers and operating systems together with software downloaded are out of date and lack security. These computers may have been infected with malware a long time ago and were never fixed by the old users.[5] Another possible cause is that, currently, whereas smartphone and tablets have become the most popular applications, their operating systems, both Android's and Apple's applications, do not have security measures equal to the

[5] <http://www.etda.or.th/etda_website/files/system/ThaiCERT_Annual_Report_th_2013.pdf>, page 47.

operating systems on desktop computers. Therefore, these portable devices are being attacked first by cybercriminals.[6] Consequently, according to reported statistics from multiple sources, Thailand was identified as a high-risk country. In the report of the "World Competitiveness Ranking 2013" issued by the International Institute for Management Development (IMD), which assessed cybersecurity of organizations in each member country, the cybersecurity of Thailand is ranked 48th of 60 member states and ranked 4th among the ASEAN countries behind Malaysia, Singapore and Indonesia. Additionally, the Anti-Phishing Working Group (APWG), whose mission is to counteract Phishing, reported that a high proportion of websites under Thai domain names have been hacked as a base for fraud by Phishing among websites registered under other country domain names.[7] With these aforesaid reports, the state of cybercrime in Thailand is critical, and urgent countermeasures and international cooperation are needed in order to cope with the issues. The following sections examine the prosecution of cybercrime and countermeasure against cybercrime in Thailand, respectively.

II. PROSECUTING COMPUTER-RELATED CRIMES IN THAILAND

A. The Public Prosecutor in Relation to the Power of Criminal Investigation and Inquiry

In general, agencies and organizations responsible for criminal investigation and inquiry are administrative or police officials as stipulated in section 17 and 18 of the Criminal Procedure Code B.E.2477 (1934).[8] Administrative or police official means an official vested by law with the power and duty to maintain public order; this shall include a warden, an official of the Excise Department, Customs Department, Harbor Department, an immigration officer and other officials when acting in accordance with arresting or suppressing crime. The inquiry official means an official vested by law with the power and duty to conduct an inquiry.[9] The development of the criminal investigation and inquiry progressed in 2004 when the Department of Special Investigation (DSI) under the Ministry of Justice was created by the Special Case Investigation Act B.E. 2547 (2004) amended by the Special Case Investigation Act (No.2) B.E. 2551 (2008). This new government agency is vested with the power and duty to prevent and control crime that has a devastating impact on the economy, social security and international relations. A special inquiry official is empowered to investigate a special case subject to section 21 of the Special Case Investigation Act B.E. 2547 (2004). Finally, the latest improvement of the criminal investigation and inquiry occurred in 2008 when section 20 of the Criminal Procedure Code was amended as follows:

> "Section 20.- If an offence punishable under Thai law has been committed outside the Kingdom of Thailand, the Attorney-General or the person acting for him shall be a responsible inquiry official or such duty may be assigned to any public prosecutor or inquiry official to exercise the power of inquiry on his behalf.
>
> In the case where the Attorney-General or a person acting for him assigns responsibility of holding an inquiry to any inquiry official, the Attorney-General or a person acting for him may let any public prosecutor participate the holding an inquiry together with the inquiry official.
>
> The public prosecutor assigned to be a responsible inquiry official or to hold an inquiry together with an inquiry official shall have the same power and duty as the inquiry officials do. All other power and duty provided by law shall be the public prosecutor's power and duty.
>
> In case a public prosecutor joins an inquiry official in holding an inquiry, the inquiry official shall conform with the public prosecutor's order and advice on collecting evidence.
>
> In case of necessity, the following inquiry officials shall be empowered to inquire in the period of waiting for the order of the Attorney-General or a person acting for him.
> (1) An inquiry official of the jurisdiction where an alleged offender is arrested.
> (2) An inquiry official requested by the government of other country or an injured person to punish an alleged offender.

[6] <http://www.etda.or.th/etda_website/files/system/ThaiCERT_Annual_Report_th_2013.pdf>, page 48.
[7] Ibid. page 105.
[8] Available at <http://en.wikisource.org/wiki/Criminal_Procedure_Code_of_Thailand/Provisions>.
[9] Criminal Procedure Code B.E.2477 (1934) section 2 (5) (6).

> If the public prosecutor or the responsible inquiry official in holding an inquiry, as the case may be, deems that the inquiry is completed, the opinion pursuant to Section 140, Section 141, or Section 142 shall be made and sent, together with a file, to the Attorney-General or a person acting for him."[10]

Computer-related crime investigation and inquiry under the Computer-Related Crime Act, B.E.2550 (2007), differs from the traditional criminal investigation and inquiry due to the nature of complexity of the computer-related offence mostly committed by offenders who are knowledgeable experts in the use of computers or electronic devices. In this regard, an investigator and an inquiry official who conduct the investigation and inquiry pursuant to making an arrest of the offender, as well as collecting evidence, needs to have the knowledge and expertise in computers and electronic devices in order to conduct such duty efficiently. Therefore, the Computer-Related Crime Act, B.E.2550 (2007) Chapter 2[11] has determined competent officials who shall be empowered to conduct computer-related crime investigations and searches for evidence as stipulated by the law. In addition, cybercrime is borderless and keeps on rising due to the fact that the global use of smartphones and development of cloud computing has engaged in cross-border computer networking. Therefore, the investigation and inquiry require international cooperation in criminal matters. Apart from examining the lawfulness of the investigation and inquiry, the public prosecutor also plays a key role in international mutual legal assistance in criminal matters and extradition. The Office of the Attorney-General is the central authority to facilitate requests from other nations and Thai government agencies.

Realizing how prosecuting computer-related crime differs from that of traditional crime, in 2012 the Office of the Attorney-General issued a guideline for public prosecutors in handling computer-related crime inquiry and prosecution. According to the guideline, where the computer-related offence is committed outside the Kingdom of Thailand, the Attorney–General or a person acting for him has to decide and make an order in relation to who will be responsible for holding an inquiry between the public prosecutor or the inquiry official. The decision could be one of these two choices pursuant to Section 20 of the Criminal Procedure Code.[12]

1. The Inquiry Official is Responsible for Holding the Inquiry and a Public Prosecutor is Assigned to Participate in the Inquiry

In this regard, the assigned public prosecutor has the same power and duty as the inquiry officials do and all other powers and duties provided by law shall be the public prosecutor's. Additionally, the inquiry official shall, with respect to the collection of evidence, abide by the orders and instructions of the public prosecutor.

The reason for this amendment of the law is that the investigation and inquiry under Section 20 of the Criminal Procedure Code is required to be investigated and inquired into thoroughly, lawfully and correctly within this stage of inquiry before submitting the case file to a public prosecutor in charge who will follow up with the criminal proceedings according to the Criminal Procedure Code. This is because the public prosecutor is entrusted, by the people, in his/her competence, expertise, impartiality and integrity in the criminal justice system.

2. The Public Prosecutor is Assigned to Be a Responsible Inquiry Official to Hold the Inquiry

In this regard, the public prosecutor has the same power and duty in conjunction with all other powers and duties vested in him/her by law as the inquiry officials do.

On 1 October 2013, the Office of the Attorney-General set up the Department of Investigation under the Office the Attorney-General. One of its missions is, by itself or together with an inquiry official, to conduct the criminal investigation and inquiry pursuant to Section 20 of the Criminal Procedure Code. This is a big change in the Thai Criminal Justice System from the previous one where only the inquiry official was the investigator or inquirer and the public prosecutor did not have any power to interfere during the investigation and inquiry process, just like the Crown Prosecution Service of England used to be.

[10] Criminal Procedure Code, *Translated Thai-English update (No.29) 2008 by Dr. Preecha KANEITNOOK.*

[11] Available at <http://www.it.chula.ac.th/sites/default/files/doc/Computer_Crimes_Act_B_E__2550_Eng.pdf>.

[12] Available at <http://en.wikisource.org/wiki/Criminal_Procedure_Code_of_Thailand/Provisions> (n.8)

The guideline for the public prosecutor in handling computer-related crime inquiry and prosecution has thoroughly imposed how to conduct the cybercrime investigation and inquiry in both aforesaid options. However, in both cases, the assigned public prosecutor must have a basic knowledge in regard to digital forensics applicable to tracing and identifying criminals together with how to preserve and collect digital evidence in accordance to the threshold set by the International Organization on Computer Evidence (IOCE) which, in this paper, will be shortly demonstrated.

The assigned public prosecutor needs to know methods of detecting and tracking down the person responsible for cybercrimes committed. He/she needs to know how to collect the evidence that will be used to build the case file and to be presented at trial. Furthermore, he/she must know that computer forensics engages in identifying, extracting, documenting and preserving information stored and transmitted in electronic or magnetic form known as digital evidence. Digital evidence can be visible, such as files accessible by using standard file management tools as Windows Explorer, or it can be latent such that it requires special software or techniques to locate and identify it.[13] In addition, he/she must know that only competent officials should undertake investigation, otherwise collection of evidence will contribute to the failure of the prosecution.

Digital evidence is fragile and vulnerable to damage and alteration by improper handling or examination. Collecting, preserving, documenting and examining this sort of evidence should be done with special precautions that ensure the integrity of the electronic evidence at a later stage. The room and computer where a cybercrime is committed is regarded as a crime scene and needs to be sealed off to ensure evidence is not tampered with. This practice is extended to the victim's computer as well. In early stages, the immediate surroundings of the subject devices are very critical. If the computer is on, it should be left on; if it is off, it should be left off. If the collection of evidence is mishandled and does not comply with the law, such as the legal warrant of search and seizure, the data collected can be challenged and may not be admissible evidence in court. Additionally, taking photographs of the crime scene and seizing and securing any papers, disks, flash drives, printouts and other electronic devices in the vicinity of the crime scene are very necessary as well.[14]

As for tracing and identifying criminals, the assigned public prosecutor must be able to analyse criminal acts in order to impose proper cybercrime charges. This is because each computer-related charge has different elements which means that the investigator sometimes needs to use a different approach. However, he/she needs to have basic knowledge of what information or evidence could be found from computer forensics such as Website and webpage, domain name, IP address, server, hosting server, Internet Service Provider, search engine, e-mail and e-mail header, username and password, URL, Whois, Internet browser, log file, chat logs, and social networking. This basic knowledge is necessary for tracing and identifying cybercriminals.

B. Criminal Litigation Process

When an inquiry official deems an inquiry completed, he/she will give an opinion pursuant to Section 140, Section 141 or Section 142[15] and submit it together with the case file to a public prosecutor in charge who will make the judgement as stipulated in Section 140, Section 141 or Section 143. There are many details in this process that the public prosecutor in charge has to take into account prior to making the decision on whether the indictment should be made. In this paper, just some core parts will be examined in regard to cybercrime prosecutions.

1. The Public Prosecutor Will Consider the Lawfulness of the Jurisdiction and the Power of the Investigation and Inquiry

When considering the computer-related crime offence as defined in the Computer-Related Crime Act, the public prosecutor in charge needs to take into account Section 17 of the law, which states:

"Any person committing an offence against this Act outside the Kingdom and;

[13] Scene of the Cybercrime: Computer Forensics Handbook By Ed Tittel (ed) 2002 chapter 9 (introduction).

[14] Collecting Digital Evidence of Cyber Crime: Misbah Soboohi, available at <www.academia.edu/1375440/COLLECTING_DIGITAL_EVIDENCE_OF_CYBER_CRIME>.

[15] Available at <http://en.wikisource.org/wiki/Criminal_Procedure_Code_of_Thailand/Provisions> (n.8).

(1) the offender is Thai and the government of the country where the offence has occurred or the injured party is required to be punished or;
(2) the offender is a non-citizen and the Thai government or Thai person who is an injured party or the injured party is required to be punished;
shall be penalized within the Kingdom."

In this case, the Attorney-General or a person acting for him shall be the responsible inquiry official pursuant to Section 20 of the Criminal Procedure Code and a relevant competent officer as defined in Section 18 and 19 of the Computer-Related Crime Act will have the authority to conduct an investigation and search for evidence.[16] If the public prosecutor in charge has found that the investigation of the aforesaid offence violated said provisions, he/she has to return the case file for re-opening the investigation by the competent inquiry official.

2. The Public Prosecutor in Charge Must Know What and Where the Evidence Necessary to Prove the Guilt of the Accused Is Located and How to Acquire It Lawfully and Correctly

The public prosecutor in charge needs to have the knowledge of how the computer system operates and how to use computers and programmes concerned in order to be able to correctly make a judgement whether the accused should be indicted; if so, it raises the question of how to exhibit the evidence at the court hearing. It is very essential that the public prosecutor in charge must understand the facts and elements of each related offence as to how the various steps were taken to commit the crime. Such actions, where the evidence used to prove each element of the crime is stored. The facts and the evidence acquired from the inquiry must be lawful and enough to indict the accused before the lawsuit is filed against him/her.

Although data, computer data and computer traffic data acquired from the inquiry are admissible as evidence, the public prosecutor in charge must examine whether the acquiring of the said evidence complies with Section 25 of the Computer-Related Crime Act, which stipulates:

> "Data, computer data or computer traffic data that the competent official acquired under this Act shall be admissible as evidence under the provision of the Criminal Procedure Code or other relevant law related to the investigation, however, it must not be in the way of influencing, promising, deceiving or other wrongful ways."[17]

3. Exhibiting Evidence at a Court Hearing

Presenting evidence in court is the most important of all stages of criminal prosecution. As aforesaid, the cybercrime investigation differs from a traditional crime investigation, as does the exhibiting of evidence used to prove the guilt of the accused at the court hearing.

As a matter of fact, much of the cybercrime evidence is likely to be electronic, such as computer code and network logs; a question is whether the court will be able to understand the technical evidence. In this regard, the public prosecutor in charge needs to take more time to clearly explain the facts and the evidence used to prove the elements of the crime and how to present a timeline demonstrating the defendant's involvement.

Expert testimony will possibly be essential to helping the judge understand the evidence together with how the crime was discovered, how it operated and how it caused damage to the system or the injured person. The potential experts could be network specialists, programming language experts to illustrate how malicious code was created to operate, forensic examiners and others. In addition, visual diagrams of the network and a timeline to focus the hidden events of planning and preparation together with demonstrating the involvement of the defendant is highly recommended.

C. Current Challenges for the Office of the Attorney General

Although the Office of the Attorney General has been playing a vital role in bringing cybercrime criminals to justice, it has not yet set up a particular unit or division to deal directly with this particular

[16] Available at <http://www.it.chula.ac.th/sites/default/files/doc/Computer_Crimes_Act_B_E__2550_Eng.pdf>.
[17] Available at <http://www.it.chula.ac.th/sites/default/files/doc/Computer_Crimes_Act_B_E__2550_Eng.pdf>.

issue. According to the laws regarding jurisdiction, cybercrime cases may be assigned to various departments/divisions subject to whether there are other traditional offences. However, most of the cases are submitted to the Department of Economic Crime Litigation, the Department of Intellectual Property and International Trade Litigation, or the Department of Criminal Litigation. Even though the Office of the Attorney General issued a guideline for the public prosecutor in handling the investigation and prosecution of computer-related crimes in 2012, it is relatively new and little training in this field for the public prosecutors has been organized. These issues could probably affect the performance of the public prosecutor in cybercrime prosecutions.

III. COUNTERMEASURES AGAINST CYBERCRIME

A. In General

In Thailand, ThaiCERT has played a pivotal role in developing systematic measures for securing digital infrastructures and best practices for human intervention by people who are ready to serve as soon as the threat report is received. It has also been developing human resources with expertise by providing training and granting certificates. Furthermore, it is a focal point to coordinate with other nationCERTs in building cooperation with international organizations and agencies.

B. In Cybercrime Prosecution

Because electronic evidence is susceptible to disappearing rapidly and changing easily, immediately obtaining or preserving that evidence is the first step in any cybercrime investigation. These problems are not as significant if the evidence is located within the territory of the injured state, but increasingly, it is located outside its borders. Therefore, quickly preserving and obtaining evidence abroad is more important than ever, and prosecuting cybercrimes increasingly needs cooperation from other countries. It is fortunate that substantial resources such as the G8 Subgroup on High-Tech Crime are available to give help to the member states for handling the investigation taking place overseas.

As for Thailand, currently both government and the private sector are aware of the damage that cybercrime has caused and how to handle this trend of threats. The challenges are that the investment necessary for securing the digital infrastructure is costly, and there are not enough experts in this field. This means that training should be held for developing the human resources to be ready to respond to the threats. Therefore, assistance, support, and cooperation from developing countries are desperately needed.

REPORTS OF THE COURSE

GROUP 1
EFFECTIVE CYBERCRIME LEGISLATION FROM THE PERSPECTIVE OF ENFORCEMENT PRACTICES

Chairperson	Mr. Werton Costa	(Brazil)
Co-Chairperson	Mr. Emil Gonzalez	(Panama)
Rapporteur	Mr. Joash Dache	(Kenya)
Co-Rapporteur	Ms. Kawabata Yuko	(Japan)
Members	Mr. Diabate Djakaridja	(Côte d'Ivoire)
	Mr. Ramesh Prasad Gyawali	(Nepal)
	Mr. Vincent Agusave	(Papua New Guinea)
	Mr. Jeffery Jean Baptiste	(Seychelles)
	Mr. Ihor Sekhin	(Ukraine)
	Mr. Sato Hiroyuki	(Japan)
Visiting Expert	Prof. Dr. Marco Gercke	(Germany)
Advisers	Prof. Hirose Yusuke	(UNAFEI)
	Prof. Yukawa Tsuyoshi	(UNAFEI)

I. INTRODUCTION

The First Session of the Group was called to order on 22nd May 2015 at 3:35 p.m in Seminar Group Room 2. It was presided over by Prof. Hirose with Prof. Yukawa in attendance. Mr. Costa of Brazil was nominated and approved by consensus to be Chairperson. Mr. Emil of Panama was nominated and approved as Co-Chair. Mr. Dache of Kenya was nominated and approved as Rapporteur with Ms. Kawabata of Japan as Co-Rapporteur.

After the elections, the Group had its first formal session. Based on the preliminary deliberations, the Group agreed to tackle the second part of its given theme on 'Development of Cybercrime Legislation from the Perspective of Enforcement Practices'. It was further agreed that the Group would conduct its discussions according to the following agenda: (1) a brief summary relating to the current situation of cybercrime legislation in each country; and (2) development of cybercrime legislation from the perspective of enforcement practices. It was agreed by consensus that in canvassing the two main items of the agenda, the Group would rely on the Convention on Cybercrime (Budapest Convention), similar regional approaches where relevant, seminar discussions and jurisdictional experiences as the primary working tools.

II. SUMMARY OF THE DISCUSSIONS

A. Synopsis of the Current Situation of Cybercrime Legislation in the Participating Countries

The Group had 10 members representing 9 countries. In relation to the current situation of cybercrime legislation in each country, it was noted that the circumstances surrounding this matter are different. Of the 9 countries represented, it was only Panama, Papua New Guinea (PNG), Ukraine and Japan which have signed and ratified the Convention on Cybercrime (the Budapest Convention). Panama, PNG and Ukraine—unlike Japan—have not enacted any unified or specific law on cybercrime but have provisions in their domestic Criminal Procedure and Penal Codes and other information and technology-related laws to investigate and prosecute cybercrime.

On the other hand, Brazil, Côte d'Ivoire, Nepal, Seychelles and Kenya have not ratified the Convention on Cybercrime. However, these jurisdictions have domestic legislation covering various aspects of cybercrime. Brazil and Seychelles rely on domestic Criminal Procedure and Penal Codes and a variety of other relevant legislation to investigate and prosecute cybercrime. Kenya has, in addition to its domestic Criminal Procedure and Penal Code, the Information and Communications law in which the substantive law of the Cybercrime Convention is codified. Nepal has enacted the Electronic Transactions Act and attendant regulations which deal with all forms of electronic transactions and digital signatures and make provisions to regulate various computer-based activities and punish cybercrime. Côte d'Ivoire has since 2013 enacted three relevant pieces of legislation, including a law on cybercrime, which address most of the current issues around cybercrime and related activities in accordance with the recommendations and directives of ECOWAS (a regional body).

The Group recognized that, although a majority of the countries represented have not ratified the Cybercrime Convention, the countries subscribe to other regional bodies under whose auspices there are major initiatives on harmonized regional frameworks on cybercrime. It was, however, noted that despite these fairly recent regional advances and the efforts at enacting and enforcing the relevant domestic laws, almost all the countries represented in the Group still have challenges in the investigation and prosecution of cybercrime. These challenges which are typically systemic, infrastructural and resource-based in nature vary from country to country, although there are generic aspects which may require similar approaches as will be seen later.

B. Development of Cybercrime Legislation from the Perspective of Enforcement Practices

In addressing this broad theme, the Group discussions centered on answering the following specific questions:

1. Whether or Not and How Long to Oblige Internet Service Providers to Preserve Data of Subscriber Information and Traffic Records

It was noted that Articles 16 (Expedited preservation of stored computer data) and 17 (Expedited preservation and partial disclosure of traffic data) of the Cybercrime Convention intentionally do not address the issue of data retention. Instead of an obligation to retain data, the Drafters of the Convention included provisions dealing with expedited preservation. Specifically, the Convention mandates a State Party to adopt such legislative and other measures to enable its competent authorities to order or obtain the expeditious preservation of specified computer data upon request where such data may be particularly vulnerable to loss or modification. It further requires a person in control of such data to preserve and maintain its integrity for up to a maximum of ninety days, which period may be subsequently renewed. The Convention also obliges the custodian of such data to keep confidential the undertaking of such procedures for the period of time provided for by its domestic law. The exercise of such powers and procedures are subject to Articles 14 and 15.

After discussion, it was agreed that:

(i) Subject to appropriate legal safeguards, there is a need for domestic legislation to provide for a minimum period of one year for retention of subscriber information and traffic records by Internet Service Providers (ISPs) whether or not there is suspicion of a crime. However, in enacting such domestic legislation, the EU directive prescribing a period of data retention which ranges from 6 months to 2 years and the European Court of Justice ruling that such provision would be inimical to human rights, should be borne in mind; and

(ii) The domestic legislation should further provide that in cases of investigation of cybercrime, competent authorities should apply for court orders to require the ISPs to preserve the integrity of the specific data for a period of 90 days which may be extended: (a) once for another 45 days; or (b) indefinitely for 90 days at a time; or (c) until the completion of investigations or indictment of the suspect. Caution should however be exercised in respect of the second and third options, especially if there is likely to be unreasonable delay in the investigation.

2. Whether or Not Digital Evidence is Admissible as Evidence at Trial and Under Which Conditions

The Group recognized that admissibility of electronic evidence is an important issue that should be addressed in domestic legislation as otherwise it would not be possible to effectively prosecute cybercrime in court. The Group appreciated that handling electronic evidence is a fairly challenging affair. The Group subsequently analyzed the Convention to identify provisions dealing with the admissibility of electronic evidence but realized that no such provision existed.

It was noted that the closest the Drafters of the Convention went in this regard are Articles 14 and 15 of the Convention. Specifically, the Convention provides in Article 14 (Scope of procedural provisions) that subject to Article 21, a State Party shall among other issues apply the relevant powers and procedures referred to in relation to collection of evidence in electronic form of a criminal offence. The Group was of the considered view that this provision does not address admissibility of electronic evidence per se. It was noted that Article 15 on the other hand merely provides for general conditions and safeguards relating to application of procedures and powers which include judicial or other independent supervision, grounds justifying application and limitation of the scope and the duration of such power or procedure.

The Group noted that in 2002, the Commonwealth developed in addition to the Model Law on Computer Crimes, a specific Model Law on Electronic Evidence. The Group also noted a similar approach in the Pacific Model Law, the Caribbean Model Law and the Sub-Saharan Model Law—all of which contain provisions specifically addressing the admissibility of electronic evidence.

Based on this broad analysis, the Group agreed that the conditions for admissibility of digital (electronic) evidence should be captured in special procedures provided for in domestic law. These conditions may include:

(i) Guaranteeing the authenticity, integrity and chain of custody of such evidence, and, with regard to authenticity and integrity, the evidence should where necessary be verified or authenticated by an expert witness or as may be directed by the court;

(ii) Preserving the privacy of the victims and accused person subject to exceptions which may obtain in domestic law; and

(iii) Subjecting such evidence to forensic examination.

3. Whether or Not to Regulate Internet Anonymity and Encryption (Whether or Not to Oblige Internet Users to Disclose and Register Their Identity Whenever They Connect to the Internet); Whether or Not to Oblige Suspects to Disclose Encryption Keys to Investigative Agencies Etc.)

The Group noted that there are two correlated issues at play in this question and canvassed these matters comprehensively because they touch on, among other fundamental rights, the freedom of expression and privacy of the individual. The Council of Europe's Committee of Ministers Declaration on Freedom of Communication on the Internet dated 28th May, 2003 was found by the Group to be persuasive. In Principle 7 (on Anonymity) the Declaration states that: 'In order to ensure against online surveillance and to enhance free expression of information and ideas, member states should respect the will of users of the Internet not to disclose their identity. This does not prevent member states from taking measures and cooperating in order to trace those responsible for criminal acts, in accordance with national law, the Convention for the Protection of Human Rights and Fundamental Freedoms and other international agreements in the field of justice and the police'.

The Group unanimously agreed that it is not desirable to oblige Internet users to disclose their identity not only on account of the adverse encroachment on the freedom of online expression but also due to the challenges attendant to implementation of such law if enacted. However, domestic legislation may provide for mechanisms through which users of the Internet in registered public places such as internet cafes may be required to provide their identity to the operators of such facilities and eventually to investigative authorities if needed.

On whether or not to oblige suspects to disclose encryption keys to investigative agencies and other state organs, it was observed that:

(i) most constitutions guarantee suspects the fundamental right to remain silent;

(ii) ordinarily, the burden of proof rests on the prosecution; and

(iii) most jurisdictions have laws prohibiting self-incrimination.

Based on these fundamental legal principles, it was therefore unanimously agreed that it would not be advisable to oblige suspects to disclose encryption keys to investigative agencies as encryption is one of the most important technical security aspects of electronic data. The Group was of the view that to address this complex matter, domestic legislation may authorize law enforcement agencies to use advanced forensic tools (such as key logger) since such a framework would allow internet users to encrypt data and at the same time create the possibility of accessing encryption keys by law enforcement agencies. This approach has been embedded in the Pacific, Caribbean and African Model Laws as a safeguard.

C. Trans-Border Access to Stored Computer Data with Consent or Where Publically Available (Article 32 of the Convention)

It was noted that Article 32 of the Convention addresses the issue of trans-border access to stored computer data as applicable only to State Parties. Specifically, the Article allows a State Party without the authorization of another State Party, to access publicly available information (open source) stored computer data, regardless of where the data is located geographically; or to access or receive, through a computer system in its territory, stored computer data located in another State Party, if the State Party seeking the information, obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data.

It was agreed that sub-article (a) is self-evident and poses no challenge as it relates to information or data which is publicly available (open source). With regard to sub-article (b), however, it was noted that some countries have not ratified the Convention as a consequence of the perceived wide latitude afforded by this provision. This idea is especially prevalent in countries which feel the provision undermines international law as it unduly interferes with the principle of sovereignty of the State.

It was also noted by way of example that some investigative agencies have, despite this provision, experienced inability to access information or data stored in off-shore Google servers due to Google's privacy policy.

In its deliberations, the Group noted the ambiguity inherent in this provision. It was however concluded that sub-article (b) may be interpreted as specifically relating to the release of data by consent of the person who lawfully has control of the data such as owners of off-shore servers (without the requirement of formal consent of the host state). In cases where there is no such consent, the Group recommends that State Parties to the Convention on Cybercrime use the provisions on mutual legal assistance. Countries that are not State Parties may use other international cooperation mechanisms in seeking information. The Group noted the UNTOC framework, which has been signed by over 150 countries, provides similar mechanisms with regard to organized crime and would be preferable in this regard.

D. Other Challenges Relating to Legislation from the Perspective of Enforcement Practices

It was noted that the manner in which the question was framed was capable of different interpretations. The Group, however, identified the following as the key enforcement challenges and suggested measures to address them:

(i) Lack of specialized cybercrime laws in most jurisdictions and, therefore, it would be advisable to enact such laws where non-existent or to adequately amend existing law to address cybercrime and related emerging issues;

(ii) Lack of adequate deterrent sanctions since most cybercrimes are committed by organized criminal gangs whether local or international and therefore there is need for appropriately deterrent penalties for convicted cybercriminals with attention to proportionality of the sanction;

(iii) Non-ratification of the Convention given the international nature of cybercrimes is a challenge, and therefore it is necessary to encourage States to ratify the Convention as it is the current and foremost global framework on cybercrime;

(iv) Lack of proper coordination among key state and non-state actors (such as ISPs) which may hamper investigations and proper prosecutions, and therefore it is important for a domestic legal framework to clarify procedures and arrangements for effective internal cooperation;

(v) Lack of specialized personnel to undertake investigation and prosecution of cybercrime, which therefore calls for continuous capacity building;

(vi) Prohibitive costs relating to investigations of cybercrime (finances, infrastructure, expertise, etc.) due to its trans-border nature, and therefore there is a need to encourage legislative authorities to increase budgetary allocations to government departments and agencies responsible for dealing with cybercrime; and

(vii) Lack of international cooperation frameworks especially where the State Parties have not signed mutual legal assistance treaties, and therefore there is need to encourage States to sign Mutual Legal Assistance Treaties and continued invocation and deepening of other international cooperation mechanisms between states.

(viii) However, there was no complete consensus on the challenge of lack of dedicated courts or special divisions in the existing court structure to determine cybercrime cases. The matter was therefore proposed for consideration and implementation at the country (state) level.

III. CONCLUSION

The Group discussions were conducted in an atmosphere of respect for individual professional opinion and recognition of sovereignty of the countries represented. This enabled robust exchange of ideas and experiences which provided a rich platform for the application of the lessons learned during the lectures. The contributions of the Group Adviser, Prof. Hirose, and Visiting Expert Prof. Dr. Gercke, were invaluable. The Group makes the recommendations contained in this Report (based on the requirements of the Convention on Cybercrime and other regional approaches) in the hope that the proposals will improve state capacity and ability to enhance the fight against cybercrime, which is a dangerous global phenomenon.

GROUP 2

MEASURES FOR EFFECTIVE INVESTIGATION, PROSECUTION AND ADJUDICATION OF CYBERCRIME CASES

Chairperson	Mr. CHAY Chandaravan	(Cambodia)
Co-Chairperson	Mr. Faatasi PULEIATA	(Samoa)
Rapporteur	Ms. Karla Torres CABEL	(Philippines)
Co-Rapporteur	Ms. URAOKA Naoko	(Japan)
Members	Ms. LAI Thi Thu Ha	(Viet Nam)
	Ms. Judith GOMEZ	(Panama)
	Mr. Thongchai ITTHINITIKUL	(Thailand)
	Mr. Safarbek NURALIEV	(Tajikistan)
	Mr. Arjun Prasad KOIRALA	(Nepal)
	Mr. HOSHI Takashi	(Japan)
Visiting Expert	Dr. Kim-Kwang Raymond Choo	(Australia)
Advisers	Prof. MORIYA Kazukhio	(UNAFEI)
	Prof. YUKAWA Tsuyoshi	(UNAFEI)

I. INTRODUCTION

Group 2 started its discussion on 25 May 2015. On that same date, the group elected Mr. Chay as its chairperson, Mr. Puleiata as its co-chairperson, Ms. Cabel as its rapporteur and Ms. Uraoka as its co-rapporteur. Group 2 conducted its discussion on the topic “Measures for Effective Investigation, Prosecution and Adjudication of Cybercrime Cases” by considering the following: 1) the current practices of the members’ respective countries; 2) the challenges to overcome; 3) approaches in improving said current practices and 4) measures that can be implemented to overcome the challenges and improve the current situation.

II. SUMMARY OF DISCUSSIONS

A. Effective Measures for Generating Cybercrime Leads

1. Strengthening Cyberpatrol Systems by Investigative Agencies and Facilitating the Reporting System from the Private Sector and the Public.

During the group discussion, it was observed that a majority of the participants do not have existing cyberpatrol systems in their respective countries. Said countries merely acquire cybercrime-related complaints and information through such reporting systems. However, that same group agreed that the reporting system may not be able to fully monitor and address the prevalence of cybercrime and that a more pro-active stance must be undertaken by the government, with the invaluable assistance of private stakeholders.

Meanwhile, the participants whose respective countries have cyberpatrol systems in place aver that there appears to be reluctance on the part of the private sector to voluntarily submit data records to investigators. This is because doing so may compromise their customers’ right to privacy, which would, in turn, affect their businesses. In such cases, a request or preservation order from authorities is required for the release of the information.

Either way, all participants agreed that technical skills and knowhow on the part of the investigators who receive the reports or conduct cyberpatrolling is crucial in cybercrime cases.

After much discussion, the group agreed on the following measures:

- There must be an existing law that requires service providers to furnish necessary information to authorities. Likewise, there must be regulations and measures to protect the right to privacy of the people.

- The public sector, i.e. police and prosecutors which are responsible for cyberpatrolling and/or receiving reports on cybercrime-related incidents, should be properly trained. The private sector should be acquainted with basic cybercrime knowledge, and public awareness on cybercrime should be encouraged.

- A more pro-active stance against cybercrime should be made by the government so that it will not heavily depend on reporting systems; volunteerism should be encouraged.

- Police agencies should be equipped with efficient high-tech tools.

- Cooperation between the public and private sectors should be strengthened.

- Existence of a primary agency (government body) that will monitor cybercrime cases is necessary.

- International cooperation is crucial in strengthening cyberpatrolling, reporting and investigating agencies.

B. Effective Measures for Tracing and Identifying Criminals and Preserving and Collecting Evidence

1. Tracing and Identifying Criminals and Preserving and Collecting Evidence.

A majority of the participants stated that IP addresses are necessary in cybercrime investigations and that they serve as leads in identifying the perpetrator. Some use logs stored in SIM cards and mobile phones in tracing cyber-criminals. On the other hand, tracing cybercriminals using SIM cards becomes a challenge when the cards are not registered.

The group opined that although IP addresses are available, the real challenge is determining the real perpetrator who used the computer associated with a specific IP address. This is because perpetrators currently would exploit proxy servers, TOR onion routers and applications to immediately erase access logs in advancing their malicious intent. Thus, there is a need for authorities to seek other sources of information, which would aid in identifying the perpetrators. This entails following the “money flow” using traditional investigative tools and undercover techniques.

Having discussed the respective situations and challenges encountered by each of the participating group members, the following measures were agreed upon:

- Cybercrime techniques should be regularly updated.

- Government should provide a conducive environment for international cooperation, as well as cooperation between agencies.

- The government should ensure that only specialized and competent officers are allowed to handle cybercrime investigations.

- Minimize dependence on IP addresses and consider other sources of information depending on the type of case, i.e. bank accounts, security cameras, and lease/utilities/infrastructure contracts, open sources in the Internet, etc., and to keep in mind that traditional investigation is also useful in cybercrime cases.

- SIM cards need to be registered to deter cybercriminals from using them with impunity.

- Existing police units should have on-call and available cybercrime experts.

- Authorities should be allowed extensions of time for service providers to save traffic and content data subsequent to proper request or order from responsible authorities/offices.

- Consider criminalizing tipping off suspects under investigation in order to maintain confidentiality.

2. Expedited and Proper Search, Seizure and Preservation of Digital Evidence

A majority of the participants reported that their respective countries do not have specific procedural laws for the search, seizure and preservation of digital evidence. They, however, follow their country's general law on criminal procedure with respect to gathering and preserving digital evidence.

The participants also reported a number of cybercrime challenges which their respective countries need to address. Those challenges include outdated techniques of investigators in collecting digital evidence, inadequate skills on the part of prosecutors and judges handling cybercrime cases, lack of highly skilled digital forensics experts who analyze data, absence of forensic laboratories and storage facilities and inadequate government budgets for cybercrime cases.

Since all the participants observed that there is a need to immediately secure digital data and preserve them for purposes of presenting the same in court, the group agreed on the importance of the following measures:

- Procedural laws which specifically treat digital evidence, i.e. translating digital evidence to physical evidence, should be legislated.

- Officers and investigators should maintain a high level of competency through regular training to ensure correct handling and examination of digital evidence.

- The governments of the participating member-countries should establish forensic laboratories equipped with adequate and updated forensic tools.

- Guidelines and manuals for investigation and seizure of digital evidence must be made available to officers and agents handing digital evidence.

- Informal channels between competent agencies and individuals should be considered in the investigation and prosecution of cybercrimes.

- International cooperation plays a vital role in the expedited search, seizure and preservation of digital evidence since cybercrime is borderless.

3. Cooperation Among Agencies and the Private Sector Dealing with Cybercrime or Cyber-Incident Cases

Most of the participants reported having available anti-virus software and respective computer emergency response teams (CERT) and/or computer security incident response teams (CSIRT) in their respective countries. All have Internet service providers. In this regard, Dr. Kim-Kwang Raymond Choo informed the group about FIRST, the international organization of CERTs.

During the discussion, it was opined by a majority of the members that the service providers in their countries are reluctant to cooperate with authorities and provide assistance in cybercrime investigations. This is especially true in banking institutions victimized by phishing. Similarly, cellphone companies are unwilling to relay subscriber information and mobile data to authorities. Compulsory cooperation is obtained by investigators through preservation orders and/or court orders.

The group agreed on the importance of the following measures:

- Countries without CERTs were recommended to establish an appropriate agency to deal with cybercrime.

- There should be a clear mechanism which would encourage public-private sector cooperation and voluntary cooperation on the part of the private sector, bearing in mind corporate responsibility.

- There is a need to raise public awareness.

- An effective mechanism for network monitoring, which has measures to ensure that the person's right to privacy is not violated, should be in place.

- Government agencies should be updated on cybercrime issues to be able to adequately address the dynamic nature of cybercrime.

- There should be sufficient allotment for up-to-date infrastructure in investigating and combating cybercrime.

4. International Cooperation.

All participants agreed that international cooperation is essential in the investigation, prosecution and adjudication of cybercrime cases. International cooperation between partner states is done through their respective Mutual Legal Assistance Treaties (MLATs) and collaboration with the International Criminal Police Organization (Interpol).

It was further agreed that international cooperation plays a vital role in the exchange of information and technologies and capacity building between nations. Once good rapport between countries has been established, assistance may be provided through informal channels. This is a faster way of securing volatile data vis-à-vis filing formal requests, which takes time to process.

Some of the participants reported that they have neither 24/7 contact points in their respective countries to promptly process international requests for assistance nor a central agency to monitor the same.

The group also remarked that acquisition of digital information from a non-signatory country is made more difficult since what may be considered a crime by the requesting country may not be an offence in another. In this regard, the latter country may refuse to render assistance. Thus, legislative harmonization between nations is strongly encouraged.

After considering the foregoing, the participants agreed on the points enumerated below:

- There is a need to establish a central/primary agency that deals with cybercrime investigations and receives information and requests from foreign states. This agency should also be equipped with a 24/7 contact point mechanism for the expeditious processing of requests.

- Procedures for the processing of requests should be simplified and streamlined.

- Regional and international treaties should be extended and the Convention on Cybercrime should be signed; otherwise, laws treating the collection, investigation, prosecution and adjudication of cybercrime offences should be legislated at the national level.

- International workshops, training programmes and dialogues on cybercrime are necessary.

- Use of informal channels between states is encouraged to expedite the retrieval of digital data.

- Cybercrime legislation and budget should be given priority by the country.

- There is a need for capacity building on the part of the investigators and responsible agencies not only for purposes of dealing with local cybercrime cases, but also in receiving and processing international requests for cybercrime investigations.

C. Effective Measures for Prosecution and Adjudication

1. Measures for Clear Presentation of Digital Evidence, Admissibility of Evidence and the Form of Digital Evidence at Trial

During the discussion, the participants agreed that digital evidence must be presented during trial in a language and manner understood by the presiding judge. Testimonies of expert witnesses are crucial, and prosecutors should have basic knowledge of cybercrime. Moreover, collaboration between the prosecutors and expert witnesses in the trial of cybercrime cases is a must.

Most of the members stated that they have existing laws which treat computer printouts of digital data as competent/admissible evidence. However, they should be duly authenticated and pass the scrutiny of genuineness and integrity of data. It was also observed that digital evidence is often ruled inadmissible by the court due to lapses in collection and analysis and failure to comply with the mandatory chain of custody procedures. Lack of forensic laboratories also contributes to this dilemma.

A majority of the participants follow their general rules on criminal procedure in presenting digital evidence in court. All agree, however, that the general rules on criminal procedure cannot fully address cybercrime evidence.

Since court hearings in cybercrime cases usually take years to finish, stipulation between the prosecutor and defence, with respect to presentation of expert witnesses, should be considered to expedite the proceedings. It would also help if the country has a specialized team of trained cybercrime investigators, prosecutors and judges/courts which handle cybercrime cases.

After much discussion, the group agreed on the following measures to overcome the above-stated pressing challenges and improve the current situation:

- There must be training programmes for the judiciary, prosecution and police on cybercrime laws and cases.

- Each country should have specialized cybercrime laws and procedures; digital evidence provisions should be included.

- Countries should have highly specialized and trained teams of investigators, prosecutors and courts for cybercrime cases.

- There must be available forensic laboratories, which are able to process and translate digital evidence to visible evidence.

- The trial courts must be properly equipped with projectors, monitors, computers and other facilities to be used in presenting digital evidence.

- Ordinary/traditional methods of evidence gathering and investigation should be considered especially when there is no direct evidence in cybercrime cases.

- Prepare a checklist enumerating the evidence collected and their chain of custody, relative to their collection, examination and safekeeping.

- Prosecution and expert witnesses should collaborate to be able to present digital evidence in a manner understandable by the court; expert witnesses must be able to convince the court that he or she is an expert.

- Consider marathon hearings for cybercrime cases to expedite court proceedings.

- Some of the participants suggested to consider introducing mixed-system trial procedure (inquisitorial and accusatorial/adversarial systems combined), i.e. enabling the judge to see all the evidence before trial, because of highly technical and voluminous pieces of evidence presented in cybercrime cases; while some participants, although opting to maintain their respective criminal laws/procedures, will implement additional measures to expedite court proceedings, before or during trial, of cybercrime cases, i.e. pre-trial conferences, if applicable, stipulation between prosecution and defence.

- Some participants suggested that there should be a legal presumption of guilt against an offender who uses proxy/TOR to conceal the real IP address and refuses to give his or her user name and password to access his or her information in the server. In this case, the burden of proof shifts to the offender to show otherwise.

III. CONCLUSION

Considering the foregoing, Group 2 concluded that there must be an interplay of the following general elements for the successful investigation, prosecution and adjudication of cybercrime cases: 1) capacity building of investigators, prosecutors and judges who handle cybercrime cases, including training on the use of digital forensics; 2) public awareness; 3) public and private partnerships and 4) international cooperation.

Authorities and officials should be properly trained and highly skilled. Investigators and digital forensics experts should have the ability and ingenuity to collect, preserve and process digital data. They should be updated with the latest technologies and forensic tools. Prosecutors and judges need to have specialized skills in dealing with cybercrime for better understanding of digital evidence to maintain proper and efficient investigation and trial of the cases.

On the other hand, the people should be properly briefed and educated on cybercrime law, or other similar laws, to encourage them to immediately report incidents of cybercrime to law enforcement authorities for proper action. The government should provide the public a forum where they can get immediate assistance. This will also prevent the people from falling prey to cybercriminals or being potential cybercriminals, consciously or otherwise.

Public and private partnerships must be encouraged. The government, on its own, will not be able to address the rapid turnover of technologies and pervasive effects of cybercrime. Strategic partnerships with private corporations, such as anti-virus companies, should be fostered.

More importantly, there must be international cooperation between nations. International cooperation entails sharing of best practices in cybercrime investigations, prosecution and adjudication, capacity building and technical assistance in cybercrime investigations.

However, to make international cooperation an effective tool against cybercrime, there must be legislative harmonization among nations so as not to allow cybercriminals to make good on their malicious intent without fear of prosecution to the detriment of the public in general.

GROUP 3
EFFECTIVE MEASURES FOR STRENGTHENING THE SYSTEM FOR SUPPRESSION AND PREVENTION OF CYBERCRIME

Chairperson	Ms. Tetiana Pavliukovets	(Ukraine)
Co-Chairperson	Mr. Takeru Sato	(Japan)
Rapporteur	Ms. Irene Cayetano Cena	(Philippines)
Co-Rapporteurs	Mr. Kunlay Tenzin	(Bhutan)
	Ms. Thi Khanh Nguyen	(Viet Nam)
Members	Mr. Thurain Aung	(Myanmar)
	Mr. Wasawat Chawalitthamrong	(Thailand)
	Mr. Taku Uehara	(Japan)
	Mr. Katsuya Toyama	(Japan)
Visiting Expert	Mr. Yuki Honda	(Interpol)
Adviser	Ms. Ayuko Watanabe	(UNAFEI)

I. INTRODUCTION

Group 3 of the 160th International Training Course commenced its discussion on 25 May 2015, on the topic of "Effective Measures for Strengthening the System for Suppression and Prevention of Cybercrime" . By the consensus of the group, Ms. Tetiana Pavliukovets was elected as the chairperson and Mr. Takeru Sato as the co-chairperson. The rapporteur was Ms. Irene Cayetano Cena and the co-rapporteurs were Mr. Kunlay Tenzin and Ms. Thi Khanh Nguyen. With the assigned topic, the group discussed the following issues: 1) Establishment of special organizations or units against cybercrime and measures of capacity building for criminal justice practitioners; 2) Facilitating international, regional and domestic cooperation among related agencies against cybercrime; and 3) Facilitating public-private partnership against cybercrime.

II. SUMMARY OF THE DISCUSSIONS

A. Establishment of Special Organizations or Units against Cybercrime and Measures of Capacity Building for Criminal Justice Practitioners

Most of the members of the group agreed to the idea that there is a need to establish a special unit that will cater to all cyber-related cases due to the complexity of the issue. The group came to this decision after a thorough study on the advantages and disadvantages of having a separate unit. Some of the members are not yet decided on whether to have a specific unit or not, for they believe that it will bring conflict with the other ministries' duties and functions. Also, they are still uncertain on how this special unit will be managed properly taking into consideration the requirements, such as human resources, logistics, infrastructure, etc., in order to have it operational.

For the capacity-building measures for criminal justice practitioners, the group reached a consensus that there must be two levels of training in dealing with cybercrimes. The first level is the basic knowledge for all cyber-practitioners to have a general overview and common understanding and appreciation of cybercrime, and the second is the specialized training for the experts for the conduct of cyber-crime-scene investigation. Also, the group agreed upon the idea to incorporate cyber-related courses upon recruitment of police officers to ensure that new officers, as first responders, at least know the basics on how to handle cybercrime cases and how to preserve the cybercrime scene to make the evidence admissible in courts. For those who want to pursue careers fighting cybercrime, specialized cyber-related training and certifications must be secured to make them experts in their chosen field of specialization.

B. Facilitating International, Regional and Domestic Cooperation among Related Agencies against Cybercrime

Based on brainstorming conducted by the group, there was an understanding that cooperation with investigative or prosecutorial agencies of other countries plays a very important role in the suppression and prevention of cybercrime. The establishment and utilization of a 24/7 point of contact is a very efficient and effective tool in the fight against cybercrime but this may not be legally binding depending on the nature of existing laws of each country. Instead, the group decided that there must be a hotline center to handle reports of cybercrime on a 24/7 basis in consonance with the Budapest Convention. Also this can be utilized for sharing of information among participating countries. Persons who are designated for this purpose must have a good understanding and appreciation on the complexity of cybercrime and must be familiar with the terminologies and technicalities of cyber-issues and concerns.

On the issue of cooperation between investigative agencies and digital forensic laboratories, all members of the group agreed that this forms part in the fight against cybercrime, whether the investigative agency is the police or the prosecutors or anybody involved in the investigation of cybercrime. Some of the participants deem it necessary to rely on the expertise of private institutions in the investigation of cybercrime cases, especially in the conduct of forensic examination, but some do not agree with this idea because of the issue of the chain of custody of evidence. Some members suggested that the digital forensic examinations be conducted by police officers who are qualified and certified in this aspect, but other members of the group were uncertain on this matter for it may incur additional financial support from the government. They also come up with the idea that these police officers will only make use of their knowledge for their own personal advantage and use it as a means to gain more influence in the government.

C. Facilitating Public–Private Partnership against Cybercrime

On the aspect of cooperation with internet service providers (ISPs), the group agreed that there must be an international regulation for all ISPs to be imposed by the Regional Internet Registry which manages the allocation and registration of internet number resources within a particular region. There must be a strict policy prior to the approval of business permits for these ISPs to comply with certain requirements, to include availability of large storage devices for preservation of information and pertinent data on cyber-related cases. With regard to the preservation of traffic data, the group came up with the recommendation that this information must be preserved not less than 90 days. However, for the data which are deemed necessary in the conduct of investigation on cyber-related cases, the preservation period may be extended depending on the necessity to do so. The group also considered the aspect of cooperation with telephone communication companies (TELCOs), for these entities can also contribute a lot in the suppression and prevention of cybercrime merely because some cyber-related offences are committed through the use of cellular phones. A strict regulation on the purchase and selling of SIM cards by these companies can aid investigators in the identification of perpetrators in cyber-related cases. This may threaten those cyber-offenders so that they cannot hide their real identities, and they cannot easily avoid the consequences of their misconduct in cyberspace; hence they need to think twice before committing cyber-offences.

Even though not all the members of the group have existing cooperation with cybersecurity companies and related agencies regarding the provision of investigation techniques, information and assistance, the group believes that all countries across the world must establish a Computer Emergency Response Team or a Computer Security Incident Response Team as part of the suppression and prevention measures for cybercrimes. Most of the members agreed that the response team for cyber-related cases must be handled by private companies for they have enough resources and facilities to deal with malware attacks. They have established their respective malware laboratories, state of the art equipment and expert personnel to conduct studies pertaining to cybersecurity. Some members of the group suggested that the response team must be taken care of by the government at the cabinet level for the reason that they have the administrative authority and power to handle computer security issues. All the members agree that these organizations should be in close coordination with the investigators and the private companies as well as the government for exchange of information and in depth collaboration.

All the members of the group gave detailed explanations as to the status of cooperation of their respective countries with universities and research institutes. It is worth noting that out of the seven countries represented in this group, only two have no research institutes for cybercrime in place at the moment. Even though these two countries have no existing research institutes to conduct studies on cybercrime, they agree that there is a need for the government to establish rapport with universities and research institutes to work closely and gather information that may support the fight against cybercrime. Information from these institutions may be used as a basis for conducting cybercrime investigations as well as suppression and prevention.

In enhancing public-awareness of the threat of cybercrime, several modes of advocacy were suggested by the group members to include the conduct of cyber-related seminars, training programmes and workshops for all members of the public and private sectors, most especially students who must use the Internet; dissemination of flyers, leaflets and other reference materials pertaining to cybercrime; conducting radio and television interviews with cybersecurity experts for warning the public on the implications of the use of the Internet; production of videos, infographics and manga materials related to cybercrime; conducting cybersecurity summits wherein experts are invited to share their knowledge to prevent cybercrime; regular publication of cybersecurity bulletins; making use of students as junior cyber-patrollers to gather information from the community; morale enhancement through the help of the religious sectors as part of the maintenance of the code of ethics and proper conduct; advertisement in public places with the use of posters and tarpaulins; and information dissemination through SMS from TELCOs and notices from banks and other institutions. The group firmly believes that the government has the greater responsibility in the advocacy and public awareness campaign in terms of cybercrime. But, it must be noted that this issue is not the sole responsibility of the government; each member of the community must contribute and do their share as responsible citizens in order not to become victims of cybercrime. If you want to get rid of becoming a victim of cybercrime, the best defence is to get rid of the use of the Internet and cellular phones.

III. CONCLUSION AND RECOMMENDATIONS

At the end of the discussion and thorough study on the nature and complexity of cybercrime, which is known to be borderless and transnational, the group recommends the following measures for the suppression and prevention of cybercrime:

1. Establishment of a special unit that will handle cybercrime-related matters in aid of investigation and prosecution of cybercriminals; to conduct analyses of digital evidence recovered; and to gather, evaluate and analyse modi operandi of cybercrime cases. Also, on capacity-building measures for criminal justice practitioners, there must be two levels of training: the basic training on cybercrime which aims to give a general overview and common understanding of the subject matter to all cyber-practitioners and the specialized training for the experts for the conduct of crime-scene investigation and enhancement of cybersecurity skills, as well as skills in digital forensics examination. For police officers, basic cyber-related courses should be incorporated in the course upon recruitment to have at least an overview on how to deal and conduct cybercrime-scene investigation for proper identification, seizure and handling of digital evidence, for they are expected to be the first responders. A specialized course must also be undertaken by those who want to pursue a career in cybercrime investigation and secure corresponding certifications needed to become experts not only in digital forensics but also in cybersecurity.

2. Facilitating international, regional and domestic cooperation among related agencies against cybercrime is a must. There should be mutual legal assistance treaties between and among other countries for exchange of information and sharing of intelligence reports relative to cybercrime. Also harmonization of the existing national legislation will also contribute to the fight against cybercrime, to have at least a minimum standard on the issue of dual criminality. In addition, establishment of a hotline center that will be operational 24/7 can also be utilized not only for information sharing but also for collaboration in the conduct of investigations. Informal channels may also be utilized taking into consideration the existing laws and constitutions of respective countries. Also, cooperation between investigative agencies and digital forensic laboratories will contribute in the fight against cybercrime not only in the form of sharing procedures for preservation and collection of digital evidence but also for the procedure and processes to obtain results of analyses.

3. Facilitating public-private partnership is an essential factor to consider in the suppression and prevention of cybercrime. There must be cooperation between internet service providers and the government in order to have a regulation in terms of preservation of all traffic data which should be not less than 90 days with an exception for data which are deemed necessary in the conduct of investigation on cyber-related cases, depending on the necessity of the information. Regarding cellular phones, strict regulation on the purchase and selling of SIM cards must be a prerequisite for proper identification of users, which is a very important tool in cybercrime prevention. Moreover, coopera-

tion with cybersecurity companies and related agencies regarding the provision of investigation techniques, information and assistance will be added factors to prevent the occurrence of cybercrime. All countries across the world must have a Computer Emergency Response Team or a Computer Security Incident Response Team. The responsibility for these teams should be delegated to private companies, for they have enough resources and facilities to handle cyber-related attacks. Cooperation with universities and research institutes are indeed indispensable, for these institutions can contribute to information gathering and sharing and keeping cyber-practitioners up to date in terms of cyber-related issues. And last but not least is the most significant measure in the prevention and suppression of cybercrime—the enhancement of public awareness through conducting cyber-related seminars, training programmes, workshops, cybersecurity summits, etc. for all members of the community, most especially the students who are very exposed in the world of cyberspace; production and dissemination of informative materials and cyber-bulletins in the form of flyers, leaflets, brochures, manga, SMS, notices, posters, tarpaulins, videos, infographics, etc.; conduct of radio and television interviews with experts on cyber-related matters; and conduct of cyber-patrolling to monitor any eventualities within cyberspace.

Cybercrime will persist all over the world, but the battle against it should not and must not only be managed by the governments of every country in the world. Everyone has obligations and roles in the society that can contribute to the fight against cybercrime. Let us all work together to prevent and suppress cybercrime in order to achieve a more secure and productive cyber-environment.

APPENDIX

COMMEMORATIVE PHOTOGRAPH

● 160th International Training Course

UNAFEI

The 160th International Training Course

Left to Right:

Above
Dr. Gercke (Germany), Dr. Choo (Australia)

4th Row
Ms. Kita (JICA), Ms. Itatsuda (Kitchen Staff), Ms. Odagiri (Chef), Mr. Miyagawa (Staff), Ms. Yamada (Staff), Ms. Hando (Staff), Ms. Sato (Staff), Ms. Oda (Staff), Ms. Ema (Staff), Ms. Iwakata (Staff), Mr. Ozawa (Staff), Mr. Toyoda (Staff), Mr. Endo (Staff)

3rd Row
Mr. Sato (Japan), Mr. Dache (Kenya), Mr. Sekhin (Ukraine), Mr. Chawalitthamrong (Thailand), Mr. Nuraliev (Tajikistan), Mr. Toyama (Japan), Mr. Gonzalez (Panama), Mr. Sato (Japan), Ms. Kawabata (Japan), Mr. Diabate (Cote d'Ivoire), Ms. Cabel (Philippines), Ms. Lai (Viet Nam), Ms. Pavliukovets (Ukraine)

2nd Row
Mr. Hoshi (Japan), Mr. Agusave (Papua New Guinea), Mr. Jean Baptiste (Seychelles), Mr. Tenzin (Bhutan), Mr. Koirala (Nepal), Ms. Uraoka (Japan), Mr. Aung (Myanmar), Mr. Chay (Cambodia), Mr. Puleiata (Samoa), Mr. Itthinitikul (Thailand), Mr. Costa (Brazil), Mr. Uehara (Japan), Ms. Cena (Philippines), Mr. Gyawali (Nepal), Ms. Nguyen (Viet Nam), Ms. Gomez Serrano (Panama)

1st Row
Mr. Shojima (Staff), Mr. Ando (Staff), Prof. Yukawa, Prof. Nagai, Prof. Moriya, Mr. Honda (Japan), Director Yamashita, Mr. Fernandez Lazaro (INTERPOL), Prof. Watanabe, Prof. Hirose, Prof. Akashi, Prof. Minoura, Mr. Ito (Staff), Mr. Schmid (LA)