Cybercrime in Asia: Trends and Challenges

4

Roderic Broadhurst and Lennon Y.C. Chang

4.1 Introduction

Information and communications technologies (ICT) are now part of everyday life and this is illustrated by the rapid growth of the Internet and social networks in cyberspace. Whether you are searching for travel information or buying concert tickets, you can easily perform these functions at any time and in the convenience of your own home or office. ICT has thus become an indispensable function of commerce and government. With the help of computers and the Internet, businesses are now able to provide immediate services to their customers at an unprecedented level of efficiency.

However, the Internet has also become the proverbial "double-edged sword." Along with convenience comes the inconvenience of computer crime. The Internet was originally built for research and its founding protocols were designed for in-built redundancy and openness. The rapid evolution of the computer networks that comprise the Internet from a government and research focus to the e-commerce and domestic arena has provided a gateway for offenders and deviant entrepreneurs:

> The Internet was built for research, not commerce. Its protocols were open and unsecured; it was not designed to hide. Data transmitted over this net could easily be intercepted and stolen; confidential data could not easily be protected (Lessig 1999, p. 39).

The costs of cybercrime are increasing in scale and gravity as the "industrialisation" of malicious software (or crime-ware) proliferates (Ollman 2008). For example, in 2009, the United States Internet Crime Complaint Centre received 336,655 complaints reporting a total in direct losses of USD$559.7 million (AFP 2010). Given this is an estimate based on complaints to just one Internet crime reporting service in one country, the real costs of cybercrime world-wide are considerable. In short the rapid expansion of e-commerce and the Internet has brought many benefits but also the emergence of various forms of crime that exploit the strengths and weaknesses of mass interconnectivity.

> The speed, functionality, and accessibility that create the enormous benefits of the computer age can, if not properly controlled, allow individuals and organizations to easily eavesdrop on or interfere with computer operations from remote locations for mischievous or malicious purposes, including fraud or sabotage (United States General Accounting Office 2010, p. 3).

As most cybercrimes are transnational in character, inconsistency of laws and regulations across country borders makes it especially

R. Broadhurst, Ph.D. (✉)
Australian Research Council Centre for Excellence in Security and Policing, Australian National University, Canberra, ACT, Australia
e-mail: roderic.broadhurst@anu.edu.au

L.Y.C. Chang, Ph.D.
City University of Hong Kong,
Kowloon, Hong Kong
e-mail: yclchang@cityu.edu.hk

J. Liu et al. (eds.), *Handbook of Asian Criminology*, DOI 10.1007/978-1-4614-5218-8_4,

Table 4.1 Number of Internet users in the Asia Pacific region 2011

Rank	Country	Number of Internet users 2011	% Population 2011	% Population 2002[a]
1	China	485,000,000	36.3	3.5
2	India	100,000,000	8.4	0.7
3	Japan	99,182,000	78.4	48.0
4	Indonesia	39,600,000	16.1	1.8
5	Korea, South	39,440,000	80.9	52.7
6	Philippines	29,700,000	29.2	2.5
7	Vietnam	29,268,606	32.3	0.5
8	Pakistan	20,431,000	10.9	0.3
9	Thailand	18,310,000	27.4	5.7
10	Australia	17,033,826	78.3	46.0
11	Malaysia	16,902,600	58.8	24.4
12	Taiwan	16,147,000	70.0	49.8
13	Hong Kong	4,878,713	68.5	64.1
14	Singapore	3,658,400	77.2	55.6
15	New Zealand	3,600,000	83.9	N/A
16	Sri Lanka	1,776,900	8.3	0.8
17	Bangladesh	1,735,020	1.1	0.1
18	Nepal	1,072,900	3.7	0.2
19	Laos	527,400	8.1	0.2
20	Mongolia	350,000	11.2	1.6

Source: Internet World Stats, http://www.internetworldstats.com/stats.htm (accessed 6 September 2011)
[a]Retrieved from Broadhurst (2006a)

difficult for countries to cooperate when investigating cross-border cyber crimes. As Katyal (2003, p. 180) observed, many countries will find it increasingly difficult to enforce their national laws against activities which are considered offensive or harmful to local taste or culture. The harmonisation of cyber-laws and regulations and the building of cooperation and comity among nations are vitally important countermeasures against cybercrime. The first step in that direction was the Convention on Cybercrime proposed by the Council of Europe of 2001, which provided a common legal framework on cybercrime.

4.1.1 Internet Access and the Digital Divide in Asia

In March 2011, there were an estimated 2.95 billion Internet users in the world (Miniwatts Marketing Group 2011). Among all Internet users, 45% (about 943 million Internet users) are located in the Asia and Pacific (i.e. Asia and Oceania) region. As can be seen in Table 4.1, the "digital divide" is aptly shown by the immense diversity between countries in levels of Internet participation. China has the most Internet users in the Asia and Pacific region and indeed the world and now exceeds the numbers on-line in North America. Indeed, almost half of the Internet users in the Asia and Pacific region are located in China. India, now 100 million Internet users, is second largest and, is followed by Japan, the Republic of Korea (South Korea) and the Philippines. Countries like Japan, South Korea, Taiwan, Singapore, Australia and New Zealand have over 70% of their total population on-line as internet users whereas in developing countries like India, Pakistan, Sri Lanka, Bangladesh and Nepal engage less than 10% of the population. The Philippines, Thailand, Vietnam and to a lesser extent Indonesia have also achieved significant Internet penetration and are also growing rapidly. Although China has by far the largest population of Internet "netizens," this still comprises only 31.8% of the total population and these are mostly urban users.

Compared with the proportion of Internet users in 2002, shown in Table 4.1 there has been a significant increase in all countries in the Asia and Pacific region in the past 10 years. For example, only 3.5% of the Chinese population were Internet users in 2002, but this increased to 36.3% by 2011. There was also a significant increase in other developing countries like Vietnam, the Philippines, Pakistan and India.

Along with the rapid rise of Internet use, cybercrime has also become prevalent in this region. However, of all the countries in the Asia and Pacific region only Japan has signed and ratified the Council of Europe Convention on Cybercrime. The Convention is the only multi-lateral instrument for the control of cybercrime and we discuss it further below. First we begin with a short introduction to the problem of cybercrime in Asia and compare the laws and regulations in Asian states with the provisions of the Convention. We also consider the challenges faced in developing effective cross-national policing of cybercrime in Asia.

4.2 Cybercrime and Its Impact in Asia

Given the expansion in Internet participation a drastic rise in cybercrime and information security problems has occurred in Japan, South Korea and greater China since 2005, according to private information security companies. For example, Symantec, a provider of computer security software, such as anti-virus tools, monitors and quantifies malicious computer activity that occurs on about 133 million computers that use their services (Symantec 2011). This describes malicious computer activities such as programs that are used to disrupt, damage or steal information from computer systems. These so-called "malware" or "crime-ware" computer codes usually include viruses, trojans, worms[1] and botnets[2] (IBM 2009; Trend Micro 2009; Wall 2007). Such crime-ware can also be purchased online from websites and underground forums or "dark" networks that include instructions on how to use such software. This enables the wider use of "attack toolkits" by non-technical actors, including criminal groups and may account for the increased prevalence of cybercrime. Along with this growth, the malware itself has evolved to adapt to countermeasures such as software programs designed to prevent and detect intrusions. Malware has also been developed to attack new devices such as smart phones and other digital devices (Symantec 2011).

Symantec also provides general Asian-Pacific-Japan region (APJ) Internet security reports that have ranked the impact on APJ countries from all kinds of malicious activities, including denial of service attacks (DDoS), botnet infections, phishing, spam and viruses. Their reports also indicate the origin of the attacks, such as the source of spam and the top countries hosting phishing sites.[3] According to their 2010 APJ report, Symantec found that

[1] A worm is a sub-class of a virus. Worms spread from computer to computer, but unlike a virus, can travel without any help from a person. The danger with a worm is its ability to replicate itself.

[2] A botnet is a network of individual computers infected with malware. These compromised computers are also known as zombie computers. The zombies, part of a botnet under the control of the botnet controller, can then be used as remote attack tools to facilitate the sending of spam, hosting of phishing websites, distribution of malware and mounting denial of service attacks. The most commonly used are centralised and P2P modes—hence the focus on command and control servers for a botnet that may comprise of thousands of zombies.

[3] The Symantec "APJ Internet Security Threat Report" measured malicious activity that mainly involved botnet-infected computers, bot command-and-control servers, phishing Web sites hosts, malicious code reports, spam zombies and Internet attack origins that took place or originated in each country. Rankings were based on a calculation of the mean average of the proportion of these malicious activities originating in each country (Symantec 2007a, b, 2008, 2009, 2011).

China ranked top in terms of malicious activities in the region, followed by the South Korea, India, Taiwan and Japan (see also Symantec 2011). As to the origin of attacks targeting the APJ region, Symantec detected that most attacks came from the USA, followed by China, South Korea and Japan (Symantec 2009). The overall impact of malicious activity placed the USA first, and China as the next most affected, but growing rapidly from 9% of such activity to 16% in 2010. Countries such as Brazil, India and South Korea account each for about 4% of such activity (Symantec 2011).

China also had the most botnet-infected computers detected in the APJ region for the period 2006–2010 while Taiwan was ranked second, followed by South Korea and India. Taipei was the city with the most botnet-infected computers in the region (Symantec. 2007a, b, 2008, 2009). A 2010 survey[4] conducted by Norton, an anti-virus provider, found that 83% of respondents from China experienced some form of cybercrime, including a computer virus or some form of crime-ware. This was much higher than the global average of 65%. Except for Japan which has a lower victimisation rate (36%), other countries in the Asia and Pacific region like Australia (65%), India (75%) and New Zealand (70%) are all higher than the global average (Norton 2010).

Malware like trojans and botnet programs are spread through social engineering techniques (Guenther 2001), i.e. methods of deception that create a false sense of trust, to gain "access information," for example a professional looking website mimicking a brand or service or via spam and phishing emails. Criminal groups are engaged in computer or network intrusions to obtain sensitive information such as identity and password information. This in turn can be used to undertake large-scale financial crime, and social engineering may be the preferred method of obtaining access to such data contained in digital devices/computers. The kinds of activities vary but encompass online scams and malware such as spyware, phishing, rootkits[5] and botnets. Malware infiltrates a computer system and may include viruses, worms, backdoors, keyloggers and trojans.

In online scams, the internet is used to reach potential victims by sending unsolicited messages pretending to originate from legitimate organisations in order to deceive individuals or organisations into disclosing their financial and/or personal identity information. Information obtained from "phishing" facilitates crimes such as financial fraud and identity theft. For example, a common form of phishing in China are lottery scams delivered by email or instant messenger that links the recipient to a fake website (cited in KIC 2011). The spread of malware is easier when a hacker is attuned to what is happening in a particular culture, and is aware of the current issues that help make the deception more effective. For example, some malware has been designed to target operating systems or websites using only Chinese language and often masked with appeals to patriotic sentiments (Symantec 2008).

Botnets are now widespread and targeted on financial opportunities. Botnets are the main mechanism for the commercialisation and industrialisation of cybercrime. Targets will include all kinds of digital devices (i.e. mobile phones, routers, switches and backup devices) as well as desk-top computers. The increase connectivity of digitized appliances linked to the Internet (e.g. vending machines, gas pumps, ATM's) and mobile phones to pay for such products will ensure that they are attractive targets. Mobile or smart phones also tend to be less well protected against intrusion than other digital devices. Real-time programs such as Instant Messaging are likely to a major risk as are social network sites where it seems many users assume safety and

[4] The survey includes the United States, Australia, Brazil, Canada, China, France, German, India, Italy, Japan, New Zealand, Spain, Sweden and the United Kingdom.

[5] Rootkits are cloaking technologies usually employed by other malware programs to misuse compromised systems by hiding files, registry keys and other operating system objects from diagnostic, antivirus and security programs.

privacy is inherent. A trend towards the development of semantic/human intelligence methods rather than syntactic measures is noted because human-based social engineering can obtain information in many cases where technological methods fail (Chantler and Broadhurst 2008).

Cybercrime in Asia as elsewhere may be caused by offenders or loose groups who are hacking "for fun" or ego-driven, but can include political or ideological motivation, hatred, or simply to earn a profit. However, the involvement of traditional criminal groups or new criminal networks is likely to be associated with financial deception and theft (Broadhurst and Choo 2011). However, when an attack occurs, it is often unclear who is behind the attack, where it originates or their motive (Barboza 2010). For example, Sony, the Japanese electronics group, was hacked into in April 2011 and the names, addresses, emails, birth dates, phone numbers and other information in respect of 24.6 million PC game customers were stolen from its servers (Telegraph 2011). Hackers could have earned a lot by on-selling this personal information to "carding" groups (websites and users with a focus on credit card fraud) or others who may use the stolen identity to de-fraud e-commerce enterprises. While Sony was pursuing legal action against the hacker groups "GeoHot" and "Graf_Chokolo," who allegedly hacked into their system, Sony suffered additional cyber attacks which included a distributed denial of service attack (DDoS): an attack which makes Web sites or other network services unavailable to Internet users by flooding it with traffic—from another hacking group "Anonymous"—an on-line activist and civil disobedience network. Although "Anonymous" are allegedly involved in the revenge, DDoS attacks on Sony over Sony's pursuit of "GeoHot" and "Graf_Chokolo," also alleged "Anonymous" hackers (Takahashi 2011), others argue that given denials by Anonymous that the motives were more likely profit-driven cyber criminals (Poulsen 2011). Such cases represent cybercrime where both profit and ideological reasons may be involved: the hackers saw Sony as profiteering from the Internet gaming industry.

4.2.1 Content Crime

Because of the political situations and the tensions between some countries in the Asia, cases of cybercrime with a political purpose are common. These can be seen between Taiwan and China, as well as between South and North Korea and Japan and China, as well as Pakistan and India (Broadhurst 2006a). For example, Taiwan's Ministry of National Defence was hacked and the computers in the Minister's Office and the Secretary's Office were infected with trojans and spyware in 2005 and in 2006. The National Security Bureau in Taiwan claimed that a Chinese cyber-army launched more than 3,100 attacks against Taiwanese Government systems in 2008, and this did not include attacks against the private sector (Chang 2011; Huang 2006; Xu 2009).

Similar occurrences can be seen between North and South Korea. For example, government agencies, banks and businesses in South Korea have suffered serious cyber attacks. The South Korean intelligence agency believes that these attacks were not conducted by individuals, but were prepared and staged by "certain organisations or states" and that North Korea was the main suspect (Parry 2009).

Since the risk of cybercrimes, regardless of motive or the role of organised crime, has expanded via botnets. How best to prevent cybercrime and to deter cyber criminals has become a major policy question for states and international agencies. The transnational nature of cybercrime basically requires that states enact laws to harmonise definitions of criminality and enhance mutual cooperation across states.

4.3 The Council of Europe Convention on Cybercrime: Budapest Convention

A key problem in the prosecution of cybercrime is that all the elements of the offence are rarely found in the same jurisdiction. Often the offender and the victim and even the evidence are located in different jurisdiction thus requiring a high degree of cooperation between the law enforcement agencies to investigate and prosecute (Brenner 2006). The extent that Asia has been able to address the need for such cooperation is addressed by describing the first international instrument and the role it has played in developing cybercrime law in Asia.

The Council of Europe's (CoE) 2001 *Convention on Cybercrime*, often referred to as the *Budapest Convention*[6] is currently the only multi-national agreement that provides for the means to prosecute cybercriminals and represents an important attempt to regulate cyberspace. In order to harmonise criminal law and procedures across the states of Europe for the prosecution of cyber-criminals, the CoE[7] drafted a convention on cybercrime. The initiative can be traced back to 1989 when the CoE published a set of recommendations on the need for substantive criminal law to criminalise harmful conduct committed through computer networks. In 1997 the CoE formed a Committee of Experts on Crime in Cyberspace to draft a convention to facilitate States' cooperation in investigating and prosecuting computer crimes and to provide a solution to cybercrime problems through the adoption of an international legal instrument (Council of Europe 2001a, b; ITU 2009; Keyser 2003; Weber 2003). In November 2001, the *Convention on Cybercrime* was opened for signature and it entered into force on July 1, 2004 after ratification by the required minimum five member countries.[8]

The Budapest Convention is supported by the United Nations (UN) and because it also included non-Council states it can be also regarded as an international, rather than regional, treaty (Archick 2006; Csonka 2000; Keyser 2003; Weber 2003). Resolution 56/121, of the UN General Assembly noted the work of international and regional organisations in combating hi-technology crime, and stressed the importance of the *Convention on Cybercrime*. The UN also invited Member States, when developing national laws, policy and practices aimed at combating the criminal misuse of information technologies, to take into account the work and "achievements" of other international and regional agreements such as the Convention (United Nations 2002).

The CoE *Convention on Cybercrime* (hereafter the Convention) has four parts: Chapter I defines the terms used; Chapter II the measures to be taken at the national level, including substantive criminal law and procedural law; Chapter III establishes the general principles of international cooperation and mutual assistance and Chapter IV includes miscellaneous matters such as accession to the Convention.[9]

In terms of substantive laws, the Convention lists four: (1) offences against the confidentiality, integrity and availability of computer data and systems, such as illegal access of a computer system; interception of non-public transmissions of computer data to, from, or within a computer system; interference with computer data; interference with computer systems, such as computer sabotage and the misuse of computer-related devices (e.g. "hacker tools"), (2) computer-related offences, including the traditional offences of fraud and forgery when carried out through a computer system, (3) content-related offences, in order to control the use of computer systems as vehicles for the sexual exploitation of children and acts of a racist or xenophobic nature and (4) offences relating to infringement of copyright and related rights.

The procedural part of the Convention aims to enable the prosecution of computer crime by establishing common procedural rules and adapting

[6] Budapest was the city in which the Convention was opened for signature November 8, 2001.

[7] The Council of Europe (CoE), founded in 1949, comprises 45 countries, including the members of the European Union (a separate entity), as well as countries from Central and Eastern Europe. Headquartered in Strasbourg, France, the CoE was formed as a vehicle for integration in Europe, and its aims include agreements and common actions in economic, social, cultural, legal and administrative matters.

[8] Only after ratification by five states (including at least three from members of the CoE) will the Convention enter into force. Albania, Croatia, Estonia, Hungry and Lithuania were the first five states to ratify the Convention.

[9] For more detail description and discussion of the Convention, please see Weber (2003) and Broadhurst (2006b).

traditional crime fighting measures such as search and seizure, and it also creates new measures, such as expedited preservation of data. As data in cyberspace is dynamic, other evidence collection methods relevant to telecommunications (such as real-time collection of traffic data and interception of content data) have also been adapted to permit the collection of electronic data during the process of communication by police or service providers. The real-time collection of traffic data and interception of content data are the most intrusive powers in the Convention (Csonka 2000). The definition of "computer system" in the Convention does not restrict the manner in which the devices or group of devices may be interconnected. These interception powers therefore also apply to communications transmitted by means of any computer system, which could include transmission of the communication through telecommunication networks before it is received by another computer system.

The Convention also makes it clear that international cooperation is to be provided among contracting states "to the widest extent possible." This principle requires them to provide extensive cooperation and to minimise impediments to the rapid flow of information and evidence. The Convention also creates the legal basis for an international computer crime assistance network, i.e. a network of national contact points permanently available (the "24/7 network"). The network established by the Convention is based on experience gained from the network created by the G8 and co-ordinated by the US Department of Justice. Under the Convention, States are obligated to designate a point of contact available 24 h a day, 7 days a week, in order to ensure immediate assistance to investigations within the scope of the Convention. The establishment of this network is one of the most important provisions provided by the Convention to ensure that States can respond effectively to the law enforcement challenges posed by computer crime.

The Convention [Article 6(1)(a)] also prohibits "…the production, sale, procurement for use, import, distribution" of software programs with the purpose of committing crime. The intention of this provision was to prevent the crimes potentially associated with these tools by banning their creation and distribution. Use and possession are also criminalised. However, if the purpose of the program was for a legitimate purpose such as "authorised testing or protection of a computer system" then possession of such "malware" was not criminalised [Article 6(2)]. An exemption similar to the possession of certain pharmaceuticals by medical practitioners for "legitimate" use, and exceptions for forensic and preventative use was also envisaged. So legitimate industry professionals are not adversely affected but has proven a difficult law to implement, and each jurisdiction can determine what sorts of malware might trigger unlawful use. Attempts have been made to control the use of these tools in Germany (German Criminal Code Law 202c 2007), the UK, (Section 37, UK Computer Misuse Act amendment effective 2008), Taiwan (Article 362, Criminal Code) and to some extent in China (Criminal Code 7th amendment in 2009—Article 285) and Japan (June 2011 Article 168-2 Japanese Criminal Code). In July 2011 a European Union (EU) ministerial meeting proposed to make "hacking tools" illegal but the definition of a "tool" has been questioned as well as the effectiveness of such a prohibition. To date, there have been few prosecutions in jurisdictions with relevant legislation, and crime-ware is still readily available.

The continued proliferation of malware arises in part because some states continue to be the "weakest links" in the supposedly seamless cross-national security web necessary to prevent cybercrime. Indeed the involvement of the state or at least quasi-state actors in the dissemination and use of crime-ware is a considerable impediment to effective law enforcement. In some countries in Asia, the absence of appropriate laws and/or effective law enforcement enables their jurisdiction to provide safe havens for cybercriminals.

4.4 Application of the Budapest Convention in Asia

As in September 2012, the Convention has received 47 signatories and of those, 37 countries have ratified it after signing. The rapid ascension of the Convention reflects the importance of the problem and the recognition that a multi-national approach will be needed. Most of the signatory countries are Member States of the CoE with only four non-member States (Canada, Japan, South Africa and the USA) signing the Convention. The USA was the first non-member State to ratify the Convention, however, the additional protocol to the convention which specifically address hate crime was excluded on the constitutional grounds of the right to free speech. The accession by the USA elevated the status of the Convention to an international rather than a regional treaty.

As noted, most countries in Asia are not signatories of the Convention. Although the convention is open to any non-member state wishing to join only Japan has signed the treat while Australia is likely to accede in late 2012 as the relevant Bill has passed in Senate in August 2012 (Lee 2012). Nevertheless many Asian countries have looked to the Convention for guidance on new laws.

Using the Convention as a benchmark, Microsoft (2007) investigated 14 countries[10] in Asia to see whether their computer security laws aligned with the requirements of the Convention. It shows that, in 2007, most countries in Asia could be classified as having either favourable alignment or moderate alignment. Only India and Indonesia were at that time classified as having a weak alignment. Since the Microsoft report, new laws against cybercrime have been introduced by PR China, India, Indonesia and Japan. These changes make the laws in those countries more closely aligned to the essential requirements of the Convention.

For example, amendments to the "Information Technology Act (IT Act), 2000" (India IT Act 2000) were adopted by the Parliament of India and ratified on February 5, 2009. The "Information Technology (Amendment) Act, 2008" (IT Act 2008) reflected largely the requirements of the Convention (Council of Europe 2009). Apart from unauthorised access, introduction of viruses, damage, disruption and denial of access in section 43 of the India IT Act 2000, the amendments also criminalised offences, such as using computer codes or communication devices to disseminate false information, dishonestly receiving or retaining any stolen computer resources or communication devices, fraudulently or dishonestly making use of electronic signature, password or other unique identification features of any other person (see amendments to section 66—66A to 66F). Also amendments to section 67, enhanced the punishment for publishing or transmitting obscene material in electronic form from 3 to 5 years and also impose fines from 100,000 to 500,000 Indian Rupees (approximately USD2,000–10,000). In addition, ancillary offences in the draft Right to Privacy Bill now before the Indian Parliament includes provisions against illegal interception (Venkatesan 2011). These amendments and new laws make India more aligned to the requirements of the Convention.

The Indonesian government enacted Law No. 11 of 2008 regarding Information and Electronic Transactions. It passed substantive laws similar to the Convention, including illegal access, illegal interception, data interference, misuse of devices, computer-related fraud and forgery (Noor 2010). China and Japan also amended their cybercrime laws, which aligned them more to the Convention. In China, the offence of illegal access only applied to the access to computer systems used for state affairs, at national defence facilities and in the aid of sophisticated scientific work. This was widely criticised as inadequate. Consequently, Amendment VII of the PRC Criminal Law was promulgated in February 2009, corrected this deficiency and illegal access to a computer system in areas other than those previously proscribed could be sanctioned (Article 285). The amendment also added sanctions for those who provide a tool or process, which is solely used for illegal access and unlawful control of a computer system in section 3 of Article 285—in effect potentially criminalising crime-ware.

[10] The countries investigated include Australia, China, Hong Kong, India, Indonesia, Japan, Malaysia, New Zealand, Philippines, Singapore, South Korea, Taiwan, Thailand and Vietnam.

In 2009 Japan revised its Penal Code to further address problems of cybercrime paving the way for ascension to the Convention. The revision made punishable the creation or distribution of a computer virus, acquisition or storage of a virus, and sending emails containing pornography images to random groups of people. The amendments also strengthened investigative powers by permitting data to be seized or copied from computer servers that are connected via online networks to a computer seized for investigation. Authorities are also given the power to request Internet service providers to retain communications logs, such as the names of email senders and recipients, for up to 60 days (Kyodo 2011).

From the discussion above, we can see that countries in Asia are not only amending their laws to regulate offences against the confidentiality, integrity and availability of computer data and systems, content offences are also a focus. Publishing or transmitting obscene material (especially obscene material involving a child) is now punishable in most Asian countries.

However, there is still little consensus on what constitutes content crime within the very diverse Asian region. It has been observed that, in Asia, notions of obscenity and pornography/erotica vary widely from country to country. For example, compared to people in China, Taiwan and Hong Kong, the Japanese might have a higher tolerance to erotic materials. Islamic countries have a much less tolerant approach to obscene materials. Many have a "zero tolerance" approach where any form of nudity is recognised as being obscene (Broadhurst 2006a).

Many countries (e.g. Australia, Italy, Norway, Sweden, Switzerland, United Kingdom, China, Iran, Saudi Arabia, Burma, Vietnam, Singapore and Thailand) attempt to exercise control over undesirable or illegal content by blacklisting websites. Although there is near universal criminalisation of child pornography, most Internet content crime, including those designed to incite racial or religious vilification crime are not criminalised. Some countries (e.g. China, Singapore, Pakistan) also filter social networking sites; however, it is also evident that many attempts at blocking or filtering web access can be readily overcome (OpenNet 2010).

In summary, laws against cybercrime in most countries in Asia are either favourably or moderately aligned with the Convention. However, dilemmas still exists when it comes to the interpretation of certain types of content crime, and it is likely that Asian countries (like the USA) may only join the convention with exceptions to the protocols on content crime.

4.4.1 The Development of the Budapest Convention

Although the *Convention* is widely considered to be the first international convention on cybercrime, and is accepted as such by the UN, some countries regard it as a regional rather than international treaty. Harley (2010) argued that, although the Convention is not strictly a regional agreement, it is also not a global convention as there is only one non-Member state of the CoE (the USA) which has ratified the Convention.[11]

The degree of participation of countries in Asia region in the *Convention* is limited, and many countries have yet to fully develop their cybercrime laws to the requisite standard. For example, differences between Chinese laws and the Convention may be the reason why China has not signed the Convention. Although recent amendments to its criminal laws have made China's legal responses to cybercrime more aligned to those of the Convention, there still remains inconsistency between Chinese criminal procedural law and the requirements of the Convention, especially in regard to search and seizure for the collection and production of computer data.

Countries such as China, Russia and India were not involved in the development of the Convention and have at times argued that a UN treaty or code would be more appropriate. This seems to be reflected by a senior police officer from China who stated (cited in Chang 2012):

> …the Council of Europe has been in contact with China, trying to persuade China to amend its law to fit the requirements of the Convention. However,

[11] Japan has ratified the Convention on July 3, 2012.

> China did not care much about this issue then. And, anyway, when they were drafting the convention, they did not invite China to join in the drafting. Now they want us to join, we are not interested.

In contrast the Taiwanese Government has expressed an interest in signing the Convention on Cybercrime, but is hindered by its ambiguous political situation, where it is not recognised by the Council of Europe as a country (Chang 2012).

Given the limited degree of participation of countries in Asia in the Convention, China along with India, South Korea, and a number of other developing countries recently initiated a proposal to create a new global cybercrime treaty. More than 50% of the world's population, or an estimated 40% of all Internet users, do not come under the auspices of the CoE Convention.

The CoE's cybercrime convention needs to be expanded or re-invented to capture the phenomenal growth of the Internet especially in Asia. Previous attempts to develop a UN convention on cybercrime may also need to be re-activated as circumstances have changed considerably since the late 1990s when the CoE began the lengthy process of creating the convention through diplomatic and expert dialogue. The absence of effective regional mutual legal assistance and cooperation in criminal matters in ASEAN and wider Asia (Gordon 2009), especially cybercrime (Thomas 2009) may be addressed via another iteration of the convention engaging those parties not originally at the table.

For some developing countries, the 2002 Commonwealth Nations model law on computer-related crime and international cooperation provides guidance especially useful for those jurisdictions sharing a common legal history. Indeed it had been estimated that over a thousand bilateral treaties between Commonwealth States are required to ensure adequate mutual legal assistance (United Nations 2010).

Developing countries may be reluctant to sign on to the CoE convention because of the high standards of procedural law and cooperation required. The depth of the digital divide and the difficulties of creating consensus should not be over-estimated in the context of a UN sponsored process. Fears among the advanced technological states that a UN instrument might result in a "dumb" down version of the CoE convention will have to be addressed in order to re-activate a more widely accepted treaty format (Masters 2010). The reluctance of Brazil to sign on to the CoE convention due to concerns about the criminalization of intellectual property (Harley 2010), however, shows that agreement will not be possible on all issues. Traditions of dual criminality in mutual legal assistance matters will remain a significant hurdle and a hybrid or two-tiered universal or UN treaty in tandem with the CoE may emerge. A global convention on cybercrime was given further impetus by the recent recommendation of the 12th United Nations Congress on Crime Prevention and Criminal Justice (United Nations 2010, para 32). Given harmonisation of responses to non-traditional security threats is relatively novel, the CoE and Commonwealth examples will be useful guides to a truly universal treaty.

4.5 Future Developments in Cybercrime Law

As the Convention is based on the types of cybercrime that originated in the late 1990s, a number of new problems and attack methods are not explicitly covered by the Convention, and these will require attention in future iterations. These include the following.

4.5.1 Botnets

The use of botnets is arguably the most significant development in cybercrime to arise since the original signing of the Convention. Using large numbers of networked infected-computers, botnet operators can launch highly damaging attacks, including such serious crimes as DDoS attacks. It can also be used to send out massive numbers of spam and phishing messages. It is estimated that 80% of phishing incidents are related to botnets (Schjolberg and Ghernaouti-Helie 2011). Large botnets with hundreds of thousands of computers have been discovered, and these have been employed for purposes of cyber-terrorism and cyber-warfare. Botnets may mimic in some ways a form of cyber-organised crime (Chang 2012).

Using bot-infected computers as springboards to launch cyber attacks, criminals can avoid investigation or disturb investigation as the compromised computers are usually located in different countries and there are still no guidelines for international cooperation on investigation. Botnets are now available for lease or purchase and can be obtained on-line for a reasonable price. Criminals without a technology background are able to launch cyber-attacks by using readily available malicious toolkits or they hire hackers to do so. As bot-infected computers' sellers and buyers can potentially be located in different countries, real-time cross-border cooperation in criminal investigation becomes essential.

4.5.2 Cloud Computing

This relatively new configuration of data storage and access is a form of shared data warehousing long used by generic service providers such as "gmail" and "yahoo" but brings new concerns in relation to cyber-security. One problem may be access to or retention of evidentiary data such as log or ISP address data, for law enforcement. "Cloud" computing provides computation, software, data access and storage services often at cheaper costs allowing users to store their data at remote storage facilities provided by service companies or to use software provided by those companies. Users no longer need to physically store their data on their own computer or buy software for themselves. While it may be convenient for users, cloud computing has the potential to become a barrier to successful crime investigation (Schjolberg 2010).

4.5.3 Anonymity and Encryption

The relative anonymity with which people conduct themselves online can lend itself to illicit activity. The use of freely available tools to mask IP addresses, locations and identities makes the task of law enforcement more difficult, as does the use of encryption programs to protect data from third party access (see Chu, Holt and Ahn 2010). While these tools also have legitimate uses, their easy availability to cyber criminals may need to be addressed in future iterations of cybercrime law. Indeed, some countries already have specific law enforcement powers to compel the release of encryption keys.

4.5.4 Social Networking

A considerable amount of cybercrime—including online harassment, stalking and child grooming—is made easier through the use of social networking sites such as Myspace and Facebook. These services are ideal for facilitating social contact and business relationships, but they also afford insufficient protection to unsophisticated and vulnerable users such as children. Greater attention to the possibilities for law enforcement monitoring of such sites, assisted by the private sector entities involved, may be required in the interests of public safety. In turn, this may necessitate a regulatory response that connects sex offenders and law enforcement databases in a more systematic way. Counter-arguments based on privacy concerns usually ignore the privacy and safety rights of victims of cybercrime.

4.5.5 A Universal Harmonised Cybercrime Law

In order to fight transnational cybercrime, it is widely agreed that there is a need for an international convention that has universal application. The EU and the USA support the CoE's *Convention on Cybercrime* and are encouraging more states to sign and ratify it. They see a process of socialising the Convention as the best way forward and are opposed to the distraction of a UN treaty and the watering down of its scope by excluding intellectual property offences, among others (USA 2011, p. 9):

> The development of norms for state conduct in cyberspace does not require a reinvention of customary international law, nor does it render existing international norms obsolete. Long-standing international norms guiding state behavior—in times of peace and conflict—also apply in cyberspace

Despite the efforts of the USA and Europe, the Convention has not reached a similar level of acceptance in other regions and countries outside the European region.

A new global cybercrime treaty was discussed at the 12th United Nation Congress on Crime Prevention and Criminal Justice in Salvador, Brazil (United Nations 2010) and a draft treaty presented by Norwegian Judge Stein Schjolberg and Professor Solange Ghernauti-Hélie from the University of Lausanne. This outlined measures similar to the Convention but took into account the criminal innovations noted above, such as phishing, bot-nets, spam, identity theft and terrorism (Schjolberg 2010). Compared with the CoE's Convention, the Draft replicated the procedural law of the convention but deleted references to intellectual property offences in cyberspace. One of the key norms and standards identified in the USA's promotion of the rule of law in the "International Strategy for Cybercrime" was the protection of intellectual property and its elimination from a proposed UN cybercrime treaty illustrated the significant differences that continue to undermine efforts to harmonise cybercrime laws. The Draft also proposed additional criminal offences such as identity theft, mass coordinated cyber-threats against critical infrastructure, terrorism and the most serious cyber-attacks including the criminalisation of crime-ware and attack toolkits. Schjolberg (2011) also proposed an international criminal court or tribunal for cyberspace because not all countries are willing to cooperate or are able to cooperate and an international criminal court or tribunal will be able to take action to investigate and prosecute transnational cyber criminals.

Russia has also sought a UN convention against cybercrime and along with China has urged the UN to adopt a voluntary code. The Russian Government has argued that the current CoE's *Convention on Cybercrime* is outdated, and did not address the problem of how to control the use of the Internet in the spread of ideas or skills relating to terrorism and cyber terrorism. Neither does the current Convention, according to this critiques put any emphasis on problems such as identity theft and the emergence of social networks and microblogs (Isakova 2011). If USA policy is any guide to the likelihood of significant changes in international approaches to cybercrime developments that restrict legitimate access to the Internet rather than combat illegal activities will be unwelcome (USA 2011, pp. 19–20).

4.6 Conclusion

This chapter briefly reviewed developments in cybercrime and the law-enforcement response in Asia. We noted the rapid rise of cybercrime as a problem and the relatively underdeveloped multilateral response to it. Although the *Budapest Convention* established a good base to harmonise the differences in laws and regulations against cybercrime between different countries, the Convention has not been widely adopted by many Asian countries or indeed as yet other parts of the world. While this may be attributable to inconsistencies with laws and regulations in some countries, for others there is reluctance to sign on to what is seen as essentially a European instrument. Even if laws are moderately or fully aligned with the Convention, they may still not wish to sign the Convention. This problem is unlikely to be solved in the near future, and may frustrate cross-national cooperation on cybercrime investigation and prosecution. With the development of new technologies such as cloud computing, "smart" phones and social media, as well as the emergence of botnets and the expansion of encryption, the Convention requires updating.

Creating a network for illegal purposes and selling or renting established botnets to commit or facilitate criminal activities along with so-called "attack toolkits" (e.g. ZeuS and Spyware) should be more widely criminalised and may help reduce organised crime in cyberspace. The widespread incidence of identity theft as a common precursor offence requires a broad-based prevention effort (Morris 2008; White and Fisher 2008). The problem of "hate" and "content" crime will remain complex and more widespread via social networks and the under-net, but with no prospect of a universal approach although prone to over-lap with criminal activity and enterprise. The potential for mitigation of transnational cybercrime ultimately lies in effective public–private partnerships and effective international cooperation, albeit not completely dependent on an international treaty (Wall 2007). Greater understanding by government and commerce of the industrial scale of commercial cybercrime, and the recognition of a sense of "shared fate" in cyberspace, will quicken the development of multilateral responses and the capability for transnational crime control. Comity can be promoted if wealthy states and affected industries are prepared to fully aid those states or agencies less capable of enacting and enforcing appropriate laws. It can be argued, however, that a strict enforcement agenda is usually not feasible because of the limited capacity of the state, especially public policy agencies whose resources are usually rationed (Broadhurst 2006b). A risk is that over-regulation could stifle commercial and technological development in developing countries and those sceptical of an interventionist approach also argue that the marketplace may be able to provide more effective crime prevention measures (Newman and Clarke 2003) and efficient solutions to the problems of computer-related crime than the state.

References

AFP. (2010, March 12). *Cybercrime surge pushes 2009 losses to 559 million dollars*. Retrieved August 25, 2011, from http://www.france24.com/en/20100312-cybercrime-surge-pushes-2009-losses-559-million-dollars.

Archick, K. (2006). *Cybercrime: The Council of Europe Convention*. Washington, DC: The Library of Congress.

Barboza, D. (2010, February 1). Hacking for fun and profit in China's underworld. *The New York Times*. Retrieved 2011, from http://www.nytimes.com/2010/02/02/business/global/02hacker.html?pagewanted=all.

Brenner, S. (2006). Cybercrime jurisdiction. *Crime, Law and Social Change, 46*, 189–206.

Broadhurst, R. (2006a). Content cybercrimes: Criminality and censorship in Asia. *Indian Journal of Criminology, 34*(1&2), 11–30.

Broadhurst, R. (2006b). Developments in the global law enforcement of cyber-crime. *Policing: An International Journal of Police Strategies and Management, 29*(3), 408–433.

Broadhurst, R., & Kim-Kwang Raymond Choo. (2011). Cybercrime and on-line safety in cyberspace. In C. Smith, S. Zhang, & R. Barbaret (Eds.), *International handbook of criminology* (pp. 153–165). New York: Routledge.

Chang, L. Y. C. (2012). *Cybercrime in the Greater China Region: Regulatory Responses and Crime Prevention across the Taiwan Strait*. Cheltenham: Edward Elgar.

Chang, Y. C. (2011). Cyber conflict between Taiwan and China. *Strategic Insights, 10*(1), 26–35.

Chantler A.N., & Broadhurst, R. (2008, October 30). *Social engineering and crime prevention in cyberspace'*. Paper presented to the Korean Institute of Criminology, Seoul.

Chu, B., Holt, T. J., & Ahn, G. J. (2010). *Examining the creation, distribution, and function of malware online*. Washington, DC: National Institute of Justice, US Department of Justice.

Council of Europe. (2001a). *Convention on cybercrime*. Retrieved November 17, 2009, from http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm.

Council of Europe. (2001b). *Convention on cybercrime: Explanatory report*. Retrieved November 10, 2009, from http://conventions.coe.int/Treaty/en/Reports/Html/185.htm.

Council of Europe. (2009). *Project on cyebercrime—final report*. Strasbourg: Council of Europe.

Csonka, P. (2000). The draft Council of Europe Convention on Cybercrime: A response to the challenge of crime in the age of the Internet? *Computer Law & Security Report, 16*, 329–330.

Gordon, S. (2009). Regionalism and Cross-Border Cooperation against crime and terrorism in the Asia-Pacific. *Security Challenges, 5*(4), 75–102.

Guenther M. (2001). *Social engineering—security awareness series'; Information Warfare Site U.K.* Accessed December 20, 2006, from http://www.iwar.org.uk/comsec/resources/sa-tools/Social-Engineering.pdf.

Harley, B. (2010, March 23). A global convention on cybercrime? *Columbia Science and Technology Law Review, XI*. Retrieved July 20, 2010, from http://www.stlr.org/2010/03/a-global-convention-on-cybercrime/.

Huang, J. P. (2006, May 15). Chinese Net-army again stormed the Ministry of National Defence. *AppleDaily*. Retrieved January 10, 2011, from http://tw.nextmedia.com/applenews/article/art_id/2609544/IssueID/20060515.

IBM. (2009). *IBM Internet Security Systems X-Force 2009 mid-year trend and risk report*. Somers, NY: IBM Corporate.

Isakova, Y. (2011, July20). Russia opts for university anticybercrime convention. *Voice of Russia*. Retrieved September 7, 2011, from http://english.ruvr.ru/2011/07/20/53481702.html.

ITU. (2009). *ITU toolkit for cybercrime legislation*. Geneva: International Telecommunication Union.

Katyal, N. K. (2003). Digital architecture as crime control. *Yale Law Journal, 112*(8), 2261–2289.

Keyser, M. (2003). The Council of Europe Convention on Cybercrime. *Journal of Transnational Law and Policy, 12*(2), 287–326.

Korean Institute of Criminology. (2011, August). *Newsletter: Virtual forum against cybercrme, 2011*. www.vfac.org.

Kyodo. (2011, June 17). Domestic cybercrime bill passed. *Japan Times*. Retrieved September 6, 2011, from http://search.japantimes.co.jp/cgi-bin/nn20110617x3.html.

Lee, M. (2012). Cybercrime Bill passes Senate, set to become law. *ZDNet*. Retrieved September 17, 2012, from http://www.zdnet.com/au/cybercrime-bill-passes-senate-set-to-become-law-7000002971/.

Lessig, L. (1999). *Code and other laws of cyberspace*. New York: Basic Books.

Masters, G. (2010, April 23). Global cybercrime treaty rejected. *SC Magazine*. Retrieved September 21, 2010, from http://www.scmagazineus.com/global-cybercrime-treaty-rejected-at-un/article/16863/.

Microsoft. (2007). *Asia Pacific legislative analysis: Current and pending online safety and cybercrime laws*. Retrieved July 11, 2011, from http://www.itu.int/ITU-D/cyb/cybersecurity/docs/microsoft_asia_pacific_legislative_analysis.pdf.

Miniwatts Marketing Group. (2011). *Internet World Stats*. Retrieved August 25, 2011, from http://www.internetworldstats.com/stats.htm.

Newman, G., & Clarke, R. (2003). *Superhighway robbery: Preventing e-commerce crime*. Devon: Willan Publishing.

Noor, M. (2010). *Cyber legislation of Indonesia*. Paper presented at the Octopus Interface Conference—Cooperation against Cybercrime. Retrieved July 11, 2011, from http://unpan1.un.org/intradoc/groups/public/documents/UNGC/UNPAN040467.pdf.

Norton. (2010). *Norton cybercrime report: The human impact*. Retrieved July 25, 2011, from http://us.norton.com/theme.jsp?themeid=cybercrime_report.

Ollman, G. (2008). The evolution of commercial malware development kits and colour-by-numbers custom malware. *Computer Fraud & Security, 9*, 4–7.

OpenNet. (2010). *OpenNet Institute 2009 survey*. Accessed July 5, 2010, from http://opennet.net/research/regions/asia.

Parry, R. L. (2009). North Korea launches massive cyber attack on Seoul. *The Times*. Retrieved July 26, 2011, from http://www.timesonline.co.uk/tol/news/world/asia/article6667440.ece.

Poulsen, K. (2011, April 27). PlayStation network hack: Who did it? *Wired New*. Accessed September 28, 2011, from http://www.wired.com/threatlevel/2011/04/playstation_hack/.

Schjolberg, S. (2010). *A cyberspace treaty—a United Nations convention or protocol on cybersecurity and cybercrime (A/CONF.213/IE/7)*. Retrieved March 11, 2011, from http://www.cybercrimelaw.net/documents/UN_12th_Crime_Congress.pdf.

Schjolberg, S. (2011). *An international criminal court or tribunal for cyberspace (ICTC)*. New York: EastWest Institute.

Schjolberg, S., & Ghernaouti-Helie, S. (2011). *A global treaty on cybersecurity and cybercrime* (2nd ed.). http://www.cybercrimelaw.net/documents/A_Global_Treaty_on_Cybersecurity_and_Cybercrime,_Second_edition_2011.pdf.

Symantec. (2011, April 2011). *Symantec internet security threat report* (Vol. 16). Cupertino, CA: Symantec Corporation.

Symantec. (2007a). *Symantec APJ Internet Security Threat Report XI: Trend for July–December 06*. Cupertino, CA: Symantec Corporation.

Symantec. (2007b). *Symantec APJ Internet Security Threat Report XII: Trend for January–June 07*. Cupertino, CA: Symantec Corporation.

Symantec. (2008). *Symantec APJ Internet Security Threat Report XIII: Trend for July—December 2007*. Cupertino, CA: Symantec Corporation.

Symantec. (2009). *Symantec APJ Internet Security Threat Report XIII: Trend for 2008*. Cupertino, CA: Symantec Corporation.

Takahashi, D. (2011). *Hacktivist group Anonymous launches "payback" cyber attack on Sony*. Retrieved July 25, 2011, from http://venturebeat.com/2011/04/03/hacktivist-group-anonymous-launches-payback-cyber-attack-on-sony/.

Telegraph. (2011). Sony says 25 m more users hit in second cyber attack. *The Telegraph*. Retrieved July 25, 2011, from http://www.telegraph.co.uk/technology/sony/8489147/Sony-says-25m-more-users-hit-in-second-cyber-attack.html.

The Parliament of the Commonwealth of Australia. (2011). *Report 116 treaties tabled on 24 and 25 November 2010, 9 February and 1 March 2011*. Canberra: The Parliament of the Commonwealth of Australia.

Thomas, N. (2009). Cyber security in East Asia: Governing anarchy. *Asian Security, 5*, 1–23.

Trend Micro. (2009). *Trend micro 2008 annual threat roundup and 2009 forecast*. Cupertino, CA: Trend Micro Inc.

United Nations. (2002). *Resolution adopted by the general assembly on combating the criminal misuse of information technologies (A/RES/56/121)*. Retrieved September 25, 2009, from http://daccessdds.un.org/doc/UNDOC/GEN/N01/482/04/PDF/N0148204.pdf?OpenElement.

United Nations. (2010). *Recent developments in the use of science and technology by offenders and by competent authorities in fighting crime, including the* *case of cybercrime'*. Working paper A/CONF.213/9, UN 12th Congress on Crime Prevention and Criminal Justice, Salvador, Brazil, 12–19 April 2010 22 January 2010. Accessed July 6, 2010, from http://www.unodc.org/documents/crime-congress/12th-Crime-Congress/Documents/A_CONF.213_9/V1050382e.pdf.

United States General Accounting Office. (2010, June). *Cybersecurity: Key challenges need to be addressed to improve research and development*. Accessed July 5, 2010, from http://www.gao.gov/new.items/d10466.pdf.

United States of America. (2011, May). *International strategy for cyberspace: Prosperity, Security, and Openness in a Networked World*. White House. Accessed September 26, from www.whitehouse.org.

Venkatesan, J. (2011). Bill on 'right to privacy' in monsoon session: Moily. *The Hindu*. Retrieved July 11, 2011, from http://www.thehindu.com/news/national/article2082643.ece.

Wall, D. (2007). Policing cybercrimes: Situating the public police in networks of security within cyberspace'. *Police Practice and Research: An International Journal, 8*(2), 183–205.

Weber, A. M. (2003). The Council of Europe's convention on cybercrime. *Berkeley Technology Law Journal, 18*, 425–446.

White, M., & Fisher, C. (2008). Assessing our knowledge of identity theft: The challenges to effective prevention and control efforts. *Criminal Justice Policy Review, 19*(1), 3–24.

Xu, S. C. (2009). Over 3,100 cyber attacks towards Taiwanese Government System were originated by Chinese cyber army. *Liberty Times*. Retrieved September 21, 2010, from http://www.libertytimes.com.tw/2009/new/mar/24/today-fo2.htm.