A New Global Convention on Cybercrime

Roderic Broadhurst

Introduction

Information and communications technologies (ICT) are now crucial elements of everyday life best illustrated by the rapid growth of the Internet and social networks in cyberspace. 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. (USA Government Accounting Office 2120: 3).

Broad based long and short-term research remains a pressing priority, as is the need to develop the human capital necessary to enhance cyber-security capability and to develop technological solutions. (USA, GAO 2010: 12, 18).

Despite the near universal reach of the Internet there is yet to emerge an effective and global means of regulation. The importance of an effective regulatory regime for the Internet and related connectivity has been emphasised many times and the current climate suggests that a crucial round of negotiation is needed. New fora such as the G20 and traditional multi-lateral and regional bodies now must be harnessed to create the momentum for an international treaty on cybercrime.

In this paper I address some of the problems around the development of a universal means of controlling crime in cyberspace. I focus both on developments in Asia as the condition par excellence for a quickening of regulatory innovation and the emerging evidence of the grave risks posed by the increased role of organised criminal activity.

The fastest growth in on-line connectivity is taking place in Asia and Africa. Asia for example now accounts for 42% (764.4 million) of the worlds 1.8 billion Internet users. However, only 20% of Asians are connected compared to 53% (425.7 million) of Europeans and 73% (259 million) of North Americans, nevertheless annual growth in connectivity and in the associated markets offers considerable scope for significant growth. China now has many more Internet users than the USA but a fast take up rate but like many other nations may take a long time to reach the near universal Internet penetration rates of 90% of the population recorded in Sweden and Norway.

Many developing countries, in Asia, such as Pakistan have substantial proportions of their population now actively on-line and the 'digital divide' between nations is shown in the considerable diversity of use in Asia can be seen in Table 1. Many of these new users of the Internet will be especially vulnerable to exploitation as developing countries often lack relevant laws and the capacity of their criminal justice systems limited in countering high-tech crime.

Cybercrime: The Perfect Borderless Crime

Cybercrime is essentially a transnational crime that exploits inter-state differences and the weaknesses of mutual legal assistance practices that have evolved to counter cross-border crime (Brenner 2006). Laws governing information security are also less well developed in emerging economies, thus providing an environment in which criminal activities can be conducted at lower risk but still have an impact on advanced economies (Choo, Smith & McCusker 2007). Policing also needs to adapt to the borderless nature of cybercrime and will need to develop effect means of international cooperation. Because online offending often transcends borders, many territories can simultaneously assert jurisdiction, particularly when an attack transits multiple jurisdictions with different regimes for preserving evidence. Timely access to evidence located in one or more foreign jurisdictions may be difficult, as it requires the assistance of authorities in the relevant jurisdiction(s), who may be unwilling or unable to assist.

Countering the risks of cybercrime requires effective coordination and collaborative efforts on the part of government and the private sector. Existing legislative regimes, despite attempts at definitional 'technical neutrality', remain vulnerable in the context of new generation technologies to commit crimes (Grabosky 2007). Achieving uniformity will be an essential strategy to minimise the risk of so-called safe havens and 'jurisdiction shopping'. The need to enhance cross-border law enforcement and improve the response of the UN, Interpol and other international agencies efforts (Dandurand et al. 2007).

The extent and nature of organized criminal (OC) activities in cyberspace is unclear. Traditional crime groups have exploited cyberspace while some operate exclusively online and may never see each other. Politically motivated groups have also made use of ICT to facilitate their criminal conduct. Criminal and terrorist groups have also recognised the value of leveraging information and ICT to facilitate, or enhance the commission of crimes, and are dynamic in identifying new opportunities and ways to overcome counter-measures. The emergence of an underground economy as the source/provider of illicit information may now indicate the level of professionalism and commercialisation present in the transnational crime sector. Trends in cybercrime have shown that attacks are increasingly originating from regions where sanctions are often non-existent or operate as 'on-costs,' and enforcement is less robust.

International Response and The Digital Divide

The Council of Europe's (CoE) 2001 Convention on Cybercrime offers an important example of what needs to be done in regulating cyberspace. Its rapid adoption within Europe and by some other countries (e.g. Japan[a]) demonstrated the urgency of a universal cross-border legal framework capable of addressing the worst aspects of criminal exploitation of the Internet. The Convention offers model legislation that has been adopted by some Asian jurisdictions (e.g. Japan) and has been influential in the development of new laws in Thailand and Indonesia (Broadhurst 2006b). However, even within the European community the Russia Federation and Turkey have not joined this initiative. China a crucial player was not engaged in creating the convention and thus had less incentive to endorse a multi-lateral treaty devised by Europeans. China like Russia has also been implicated in politically motivated cyber attacks and thus may be reluctant to agree to potentially onerous investigations of cybercrime mandated by the convention.

The CoE's cybercrime convention urgently needs to be expanded or re-invented to capture the phenomenal growth of the Internet especially in Asia. Previous attempts to develop a United Nations 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 (four year) 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 Commonwealth Nations model law on computer-related crime and international cooperation (2002) 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 (UN 2010). The impact of the intended harmonization provided by the model law is limited to member states of the Commonwealth.

A review of the legislative coverage or criminalisation of cybercrime in Asia showed that many gaps continue to exist in the 'seamless web' of laws designed to

---

[a]In May 2010 Australia although a non-member state without observer status has made steps to sign the CoE treaty. As of June 2010, 30 states (including the USA one of the only nine observer states) have ratified the treaty. A further 16 states have signed but not ratified the treaty. The Additional Protocol making any publication of racist and xenophobic propaganda via computer networks a criminal offence was added to the treaty in 2006.

counter cybercrime in the region (Microsoft 2007). Microsoft used the CoE Cybercrime Convention bench-mark, and, noted the poor compliance with model privacy laws and only one jurisdiction met the modest 'opt-out' anti-spam regime CoE benchmark. Even for basic offences such as the criminalization of unauthorized access to computers, systems, programs and data some countries had yet to enact laws. Despite widespread public alarm only one jurisdiction met the model laws for on-line child safety and six countries were without relevant laws. In short the scope of legal countermeasures to cybercrime provided ample opportunity to exploit cross-border legal loopholes.

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. 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 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 Twelfth 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 UN mandated treaty. Perhaps more radically the 'securitisation' of cybercrime a process that evokes a crisis-like security context in order to permit extra-ordinary measures may be one of the few avenues for rapid adoption of a universal treaty that might help control cybercrime (Thomas 2009).

Table I: Internet Usage in Asia in 2009

Country	Internet Users	% of Population
China	384.00	28.70
Japan*	96.00	75.50
India*	81.00	7.00
South Korea	37.50	77.30
Indonesia*	30.00	12.50
Philippines	24.00	24.50

Country	Internet Users	% of Population
Vietnam	22.80	25.70
Pakistan	18.50	10.60
Australia*	17.00	80.10
Malaysia	16.90	63.70
Thailand	16.10	24.50
Taiwan	15.10	65.90
Hong Kong	4.90	69.20
Singapore	3.40	72.40
Sri Lanka*	1.20	5.50
Bangladesh	0.56	0.40
Laos	0.53	7.70
Nepal	0.50	1.70
Mongolia	0.33	10.90
Timor-Leste	0.02	0.20

Notes: Australia is included for comparison and estimates rounded to the nearest decimal and countries marked with an asterisk (*) denotes countries that have adopted the convention as a legislative guide; Central Asian states were as follows: Uzbekistan 8.9%; Azerbaijan 29.7%; Kazakhstan 14.9; Kyrgystan 15.6%; and Tajikistan 8.2%. Source http://www.internetworldstats.com/stats.htm, (accessed June 21, 2010).

Future Trends in Cybercrime and the Role of Organized Crime

Although little is known about the extent of organized criminal (OC) activity in cyberspace some trends have emerged (Council of Europe 2004). Cybercrime ranges across a spectrum of activities and behaviors that invite criminal groups: at one end are crimes that involve breaches of privacy, such as attacks on the integrity of information held in digital depositories, identity theft and the use of illegally obtained digital information. Midway are transaction-based crimes such as fraud, trafficking in child pornography, digital piracy, money laundering, and counterfeiting. At the other end of the spectrum are those crimes that involve attempts to disrupt the actual workings of the Internet. These include spamming, hacking, and denial of service attacks against specific sites to acts of cyber-terrorism by non-state actorsthat is, the use of the Internet to affect a nation's economic and technological infrastructure (Broadhurst & Chantler 2008).

Not all criminal misuse of computers or digital devices involves hacking since passwords, and other protective codes can be obtained by 'social engineering'[2]to

gain access then erase, modify or copy the information to suit the needs of their attack (Guenther 2001). The role of criminal groups in computer or network intrusions such as hacking and unauthorised access is to obtain sensitive information in order to undertake large-scale profitable crime and social engineering may be the preferred method of obtaining access among traditional OC groups. The kinds of activities vary but encompass online scams and malware such as spyware, phishing, rootkits,[3] and botnets.[4] Malware infiltrates a computer system and includes viruses, worms,[5] backdoors, keyloggers, and trojans. An example is keylogging programs that monitor user activity including keystrokes and can then be used to steal passwords or credit card details.

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' facilitate crimes such as financial fraud and identity theft. OC groups have been involved in phishing scams that target company executivesalso known as 'spear phishing' or 'whaling' in reference to bigger 'fish' (Choo & Smith 2008). OC groups also use identity fraud to conceal identities to evade detection and protect their assets from confiscation or to commit frauds and other crimes.

Botnets will become more widespread and targeted on financial reward. 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 they will be attractive targets (Chantler & Broadhurst 2008). Real-time programs such as Instant Messaging are likely to a major risk vector as are social network sites where it seems many users assume safety and privacy is inherent. A trend towards an emphasis on 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

Early accounts of 'hackers' noted a non-profit orientation, but also a likely shift to profit goals once the Internet developed (Chantler 1995). Current assumptions are that OC are profit-focused enterprises that acquire the necessary resources for cybercrime by (*inter alia*) using delinquent IT professionals and targeting weakly protected computers/networks or other digital devices. Consequently, deterrence (increased penalties and detection) is the main response enhanced by trained police (capable guardians) and target 'hardening' (Newman and Clarke 2003). However,

such an assumption in respect to some forms cybercrime may be misplaced because there is an absence of evidence-based research about offender behaviour and recruitment in cyberspace. Social learning and offender pathology may also play a significant role in predisposing some actors to criminal activity in cyberspace, where anonymity reduces social surveillance and self-control (Jayawardena & Broadhurst 2007). Ideological based criminal or terrorist groups are one form of rational non-profit motivation that requires complex regulatory

Hate and so-called 'content' crimes perpetrated via the Internet may reflect social or individual pathologies, and less the exercise of rational choice although it may be 'rational' to adopt Internet strategies of dissemination (Broadhurst 2006a). Many countries (e.g. Australia, Italy, Norway, Sweden, Switzerland, United Kingdom, China, Iran, Saudi Arabia Singapore and Thailand) attempt to exercise control over undeserbale or illegal content by blacklisting websites. Although there is near universal criminalisation of child pornography most Internet content crime, including those designed to suppress hate/racial or religous vilification crime. 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. According to an, OpenNet Institute survey in 2009 in Asia: "China, Burma, and Vietnam continued to rely on pervasive filtering practices to shape public knowledge and expression by targeting primarily content specific to politically sensitive topics in their own countries, especially Web sites in local languages" (accessed July 5, 2010, http://opennet.net/research/regions/asia).

Conclusion

Organised criminal activity in cybercrime is predicted to grow and will affect the financial security of online business and cause widespread social harm. Creating a network for illegal purposes and selling or renting established botnets to commit or facilitate criminal activities should be more widely criminalized and may help reduce organized crime in cyberspace. The widespread incidence of identity theft as a common precursor offence requires a broad-based prevention effort (Morris 2008; White & Fisher 2008). The problem of "hate" and "content" crime will become more complex and widespread via social networks and the under-net with little prospect of a universal approach but 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 (Wall 2007). Greater knowledge of the scale of 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.

1. That is: Australia, Hong Kong, New Zealand, India, Taiwan, China, Japan, Vietnam, Malaysia, South Korea, Philippines, Indonesia, Thailand and Singapore.

2. The term used to describe the use of psychological tricks and the manipulation of behaviour often by means of deception, by cyber-criminals on unsuspecting users to gain 'access information' in order to commit crime.

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

4. A botnet is a network of individual computers infected with bot malware. These compromised computers are also known as zombies or 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. P2P and randomthe most commonly used are centralised and P2P modes

5. A worm is similar to a virus by design, and is considered to be a sub-class of a virus. Worms spread from computer to computer, but unlike a virus, have the ability to travel without any help from a person. The danger with a worm is its ability to replicate itself on your system, so rather than your computer sending out a single worm, it could send out hundreds or thousands of copies of itself, creating a huge and devastating effect.

References

Brenner S (2006) 'Cybercrime Jurisdiction', *Crime, Law and Social Change*, 46: 189-206.

Broadhurst, R.G. (2006a) 'Content Cybercrimes: Criminality and Censorship in Asia', *Indian Journal of Criminology*, 34 (1&2):11-30.

Broadhurst, R.G. (2006) 'Developments in the Global Law Enforcement of Cyber-Crime', *Policing: An International Journal of Police Strategies and Management*, 29:3, 408-433.

Chantler A.N. & R. Broadhurst. (2008) Social Engineering and Crime Prevention in Cyberspace', paper presented to the Korean Institute of Criminology, October 30, 2008, Seoul.

Choo KKR (2008) 'Organized Crime Groups in Cyberspace: A Typology', *Trends in Organized Crime* 11:3, 270295.

Choo KRR, Smith RG & McCusker R. (2007) *Future Directions in Technology-Enabled Crime: 2007-09*. Research and public policy series no. 78. Canberra: Australian Institute of Criminology. Online. Available HTTP: http://www.aic.gov.au/publications/current%20series/rpp/61-80/rpp78.aspx (accessed 31 July 2009).

Choo, KKR and RG Smith. (2008) 'Criminal Exploitation of Online Systems by Organized Crime Groups', *Asian Journal of Criminology*, 3:1, 3759.

Council of Europe. (2004) 'Summary of the Organized Crime Situation Report: Focus on Cybercrime', Octopus Interface conference: Challenge of Cybercrime, September 15-17, Strasbourg

Council of Europe (2001), 'Convention on Cybercrime CETS No.185', see

http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CL=ENG. (accessed 21 June, 2010).

Dandurand Y, Colombo G & Passas N. (2007) 'Measures and Mechanisms to Strengthen International Cooperation among Prosecution Services', *Crime, Law and Social Change*, 47:45, 261289.

Gordon, Sandy (2009). 'Regionalism and Cross-Border Cooperation against Crime and Terrorism in the Asia-Pacific', *Security Challenges*, Vol. 5, No. 4, (Summer 2009), pp 75-102.

Grabosky, P. (2007) 'The Internet, Technology and Organized Crime', *Asian Journal of Criminology*, 2:145-162.

Harley, Brian, 'A Global Convention on Cybercrime?' Columbia Science and Technology Law Review, Volume XI, 2010, March 23, 2010. see http://www.stlr.org/2010/03/a-global-convention-on-cybercrime/ (accessed 21, June 2010)

Guenther M. (2001) 'Social Engineering Security Awareness Series'; Information Warfare Site U.K. Online. Available HTTP: (http://www.iwar.org.uk/comsec/resources/sa-tools/Social-Engineering.pdf) (accessed 20 Dec 2006).

Jayawardena, K. and R. Broadhurst. (2007) 'Online Child Sex Solicitation: Exploring the Feasibility of a Research 'Sting'', *International Journal of Cyber Criminology*, 1:2.

MicroSoft. (2007) Asia Pacific Legislative Analysis: Current and Pending Online Safety and Cybercrime Laws. A Study by Microsoft, November 2007, Online. Available HTTP: http://www.itu.int/ITU-D/cyb/cybersecurity/docs/microsoft_asia_pacific_legislative_analysis.pdf (accessed 31 July 2009).

Morris, S. (2004) 'The Future of Netcrime Now: Part 1 Threats and Challenges', Home Office [UK] Online. Available HTTP:http://www.homeoffice.gov.uk/rds/pdfs04/rdsolr6204.pdf (accessed 31 July 2009).

Newman, G. & R. Clarke. (2003) *Superhighway Robbery: Preventing E-commerce Crime*. Devon: Willan Publishing.

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) http://www.unodc.org/documents/crime-congress/12th-Crime-Congress/Documents/A_CONF.213_9/V1050382e.pdf

United Stated General Accounting Office 2010, 'Cybersecurity: Key Challenges Need to Be Addressed to Improve Research and Development', June 2010: http://www.gao.gov/new.items/d10466.pdf (accessed July 5, 2010:)

Thomas, N. (2009) 'Cyber Security in East Asia: Governing Anarchy', *Asian Security* 5, 1-23.

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.

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.

The author Roderic Broadhurst is Professor at Australian Research Council, Centre for Excellence in Policing and Security, Regulatory Network, School of Regulation, Justice and Diplomacy College of Asia Pacific, Australian National University. He can be reached at roderic.broadhurst@anu.edu.au.