Developments in the global law enforcement of cyber-crime

[Revision 7.1.06 – 13256 words]

Roderic Broadhurst, Queensland University of Technology *

Policing*: *An International Journal of Police Strategies and Management
29(2) : pp. 408-433.

Copyright 2006 Emerald

*PhD., Professor, email: r.broadhurst@qut.edu.au.

Developments in the global law enforcement of cyber-crime

Abstract

The rapid expansion of computer connectivity has provided opportunities for criminals to exploit security vulnerabilities in the on-line environment. Most detrimental are malicious and exploit codes that interrupt computer operations on a global scale and along with other cyber-crimes threaten e-commerce. Cyber-crime is often traditional crime (e.g. fraud, identify theft, child pornography) albeit executed swiftly and to vast numbers of potential victims, as well as unauthorised access, damage and interference to computer systems. The cross-national nature of most computer related crimes have rendered many time-honoured methods of policing both domestically and in cross-border situations ineffective even in advanced nations, while the 'digital divide' provides 'safe havens' for cyber-criminals. In response to the threat of cyber-crime there is an urgent need to reform methods of mutual legal assistance and to develop trans-national policing capability. The international response is briefly outlined in the context of the United Nations Transnational Organised Crime Convention (in force from September 2003) and the Council of Europe's innovative Cybercrime Convention (in force from July 2004). In addition the role of the United Nations, Interpol, other institutions and bi-lateral, regional and other efforts aimed a creating a seamless web of enforcement against cyber-criminals are described. The potential for potent global enforcement mechanisms are discussed.

Key words: computer related crime; cyber-crime; transnational crime; Council of Europe Cybercrime Convention, crime prevention; and mutual legal assistance

Introduction

The rapid development of computer connectivity and the role of the Internet in the emergence of new e-commerce have compelled national governments and international agencies to address the need for regulation and safety on the 'information superhighways'. These astonishing tools have eroded the traditional barriers to communication, compressed our concepts of time and place, and changed the way a large part of the world does business. The convergence of computing and communications and the exponential growth of digital technology have brought enormous benefits but with these new benefits come greater risks both domestically and across borders. The new opportunities created in 'cyberspace' have enhanced the capacity of individual offenders and criminal networks that have emerged to exploit vulnerabilities in the 'new' economy.

The role of digital and information technologies in the generation of national wealth now means that the new risks associated with these changes require continued attention on all fronts: national, regional and international. While the process of 'globalisation' continues to accelerate, a fully global response to the problems of security in the digital age has yet to emerge and efforts to secure cyberspace has been reactive rather than proactive. Developments in the trans-national policing of 'cyberspace' so essential in addressing cyber-crime are the focus of this paper and it outlines what the international community has achieved so far.

Controlling crime involving digital technology and computer networks will also require a variety of new networks: networks between police and other agencies within government, networks between police and private institutions, and networks of police across national borders. Over the past decade, considerable progress has been made within and between nations to develop the capacity of police to respond to cyber-crime and there is now growing awareness amongst computer users of the need for basic security on-line. Yet the pace of technological change will continue unabated, and the adaptability of cyber-criminals will continue to pose challenges for law enforcement. Thus the cliché 'think globally act locally' is especially pertinent in the control of cybercrime. The remarkable quickening of transnational law enforcement cooperation in response to cybercrime and other global threats has radically altered expectations about what may be achieved at the international level. As promising as this development may be what has been achieved can only be regarded as a beginning.

Until very recently it was not possible to talk about an international consensus on combating cyber-crime, especially the transnational forms it often takes. However, there is now a positive 'moral climate' for enforcement action, whether by civil, criminal or administrative measures, and this cross-border cooperation recognises what sociologists call 'communities of shared fate'. At the international level two new treaty instruments provide a sound basis for the essential cross-border law enforcement cooperation required to combat cyber crime. The first of these instruments, the Council of Europe's Cyber-crime Convention, is purpose built and although designed as a regional mechanism has global significance. The second is the United Nations Convention Against Transnational Organized Crime, which is global

in scope but indirectly deals with cyber-crime when carried out by criminal networks in relation to serious crime.

The push for a universal instrument has also gained momentum and a UN draft resolution in 2003 at the fifty-eighth session of the General Assembly on 'Cybersecurity and the protection of critical information infrastructures', (co-sponsored by Argentina, Bulgaria, Canada, Ethiopia and the United States of America), invited Member States and all relevant international organizations to take into account the need to protect critical information structures from possible misuse, including tracing attacks and, where appropriate, the disclosure of information to other nations (Redo 2004). Yet the rapid development of a purpose-built UN cyber-crime treaty is unlikely because many of the digitally advanced states prefer to extend the reach of the Council of Europe's convention to more countries, await assessment of the effectiveness of the convention, and are struggling to provide expertise to meet the demand for comprehensive counter measures including the essential mutual legal assistance (see Korean Institute of Criminology 2005, Workshop 6 'Measures to Combat Computer-related Crime' 11th UN Congress on Crime Prevention). Thus the role of agencies such as the United Nations Office of Drug Control and Crime Prevention (UNDCP) and its Centre for International Crime Prevention (CICP), Interpol, the Organisation for Economic and Cultural Development (OECD), the G8 group of nations and regional bodies such as the European Union (EU), Organisation of American States (OAS), Association of South East Asian Nations (ASEAN), and the Asia Pacific Economic Council (APEC) provide the political and technical expertise necessary to effect cross-border cooperation in policing. The web of relationships that such supra-state agencies play in responding to cybercrime is also briefly described.

Challenges

Law enforcement agencies in many jurisdictions have been unable to respond effectively to cybercrime and even in the most advanced nations, 'play catch-up' with cyber savvy criminals (Sussmann, 1999, Council for Security Cooperation Asia and Pacific, 2004). Web-page 'jacking', considered fanciful only a few years ago, is an effective way to steal a customer's identification. In December 2003 a cloned Hong Kong and Shanghai Banking Corporations' Internet banking web-page that compromised an unknown number of customers' identification illustrates this form of cyber-theft (*China Daily*, December 7, 2003:2). At the extreme of the risks now posed, cyber-criminals operating in the context of failed or failing states contribute to the criminalisation of the world economy, by providing both safe havens and plundered resources (see Gros 2003). As never before and at little cost a single offender can inflict catastrophic loss or damage on individuals, companies, and governments from the other side of the world. For example a 14-year-old Hong Kong boy was arrested for creating a false website, purportedly authorised by a well-regarded local newspaper. He posted on that website false information concerning the SARS epidemic, stating that Hong Kong would be declared a closed port. This caused widespread panic in the Hong Kong community. One consequence was supermarkets were over-run by fearful citizens stocking up on foodstuffs to tide them over the quarantine of Hong Kong. Calm was only restored some hours later when the government issued repeated public announcements denying the rumour. The 14-year-

old was convicted and placed under welfare care for 12 months (*HKSAR v Sum Cheuk Wa*, FLS 700017/2003). With these risks has come the awareness that 'information security' is no longer a matter for the technical and computer specialist, but for millions of people who now engage these new media every day for business, communications and leisure.

Forensic specialists tasked with investigating computer-related crime also face new challenges. A shift away from 'script kiddie' releases of malicious software to bespoke code designed to steal information, especially personal identification (ID) data. The greater use of encryption and access protection also poses a growing challenge of extracting evidence from computers, and servers. Another continuing problem was the reluctance of victims to report offences and that many victims are unaware that they or the computers had been compromised. The implications of such activity for infrastructure protection are ominous (Semple 2004). The online availability of source code and automated 'easy to use' hacking tools that act as system reconnaissance provide multiple exploit tools and deploy 'spy-ware' (i.e. keystroke monitoring or transmission); this had also increased the risks of computer intrusion activity as a predicate to other criminal activity such as extortion, financial or Internet fraud, identity theft, telecommunications theft, and economic espionage. Moreover, 'patch' countermeasures have proved inadequate because too many users failed to update (regardless of whether the software was licit or illicit) as 'MS blaster' demonstrated, despite the availability of an effective patch some months before the release of this particular malicious code.

Digital Divide

The 'digital divide' between nation-states is growing rapidly and the role of 'advanced' IT-based economies in bridging this divide is essential. Most developing countries do not have a telecommunications sector capable of supporting ICT. In 2000, the United Nations reported that only about 4.5% of the global population had network access, but that 44% of North Americans and 10% of Europeans did, while rates for Africa, Asia, and South America ranged from 0.3 to 1.6%. Currently, more than 98% of global Internet protocol bandwidth, at the regional level, connects to and from North America. Fifty-five countries account for 99% of worldwide spending on information technology production. A fifth of the world's people living in the highest-income countries have 86% of the world's GDP and 93% of Internet users, whereas the bottom fifth have 1% of GDP and only 0.2% of Internet users (UN 2003, cited in Redo 2004; see also Norris 2001).

Nowhere is this 'digital divide' more extreme than in Asia, with countries such as South Korea, Japan, Hong Kong and Singapore leading the way with Internet access reaching as many as 70% of households (often with broadband), while Laos, Cambodia, Mongolia and Myanmar had less than 1% of their populations connected. However, rapid growth of computer use in China has seen their number of Internet users reach 94 million at the end of 2004, exceeding Japan, Taiwan and Korea combined. Although the proportion of households connected remains relatively low at about 7.2% the total number of users will exceed the number in North America by 2008 (China Internet Network Information Center, '15th Statistical Survey Report on the Internet Development in China', January 2005 see www.cnnic.net.cn visited January 25 2005). Like other regional forums, ASEAN has recognised the need for better policing cooperation and APEC has supported the important role of e-

commerce in fostering economic development and through its ‘E Security Task Group’ (APEC Telecommunications and Information Working Group) has begun to provide guidance on a raft of issues relating to ‘e-readiness’ and governance.

Terrorism and organised crime

There is also growing concern about the potential for misuse of ICT by terrorists. This has made cyber-terrorism a major strategic issue in the prevention of terrorism because the technologies themselves may be attacked, and can also be used to support of terrorism in the same way ICTs are used by predatory cyber criminals. The use of computers by terrorists to plan, organise and communicate is well documented and counter-terrorism agencies have commonly identified high-tech media such as cellular and satellite telephones and Internet-based communications. Cases have also been reported in which hacking, physical thefts or the corruption of officials has been used to gain access to sensitive law enforcement information (see International Narcotics Control Board [INCB] 2001). The global reach of terrorism prompted the UN General Assembly in its resolution 51/210, to note the risk of terrorists using electronic or wire communication systems to carry out criminal acts (Redo 2000, 2004). The intersect between terrorism and organised crime in the post 9/11 environment have also necessitated more intrusive methods of monitoring ICT, notably the Internet and also pose significant threats to individual privacy.

The increased utilisation of data surveillance technologies focused on identity and location are based on imperfect convergence technologies that aim to merge existing and new data sources to address the problems arising from ‘asymmetric warfare’ but compel greater collaboration between the private sector and policing agencies (Levi and Wall 2004). A direct outcome of this is the stress on critical infrastructure protection. This is particularly challenging, given that most elements of critical infrastructure such as power generation, telecommunications, transport, and institutions of the financial system are owned by the private sector. The need for cooperation between law enforcement and the private sector is obvious. To help bridge the public–private gap, the United States Federal Bureau of Investigation (FBI) introduced the ‘Infraguard Program’ with over 4000 members (Iden 2003) – a programme replicated in other countries. Effective control of cyber-crime, however, requires more than cooperation between public and private security agencies. The role of the communications and IT industries in designing products that are resistant to crime and that facilitate detection and investigation is crucial.

Collaborative enforcement

The unsafe ‘highway’ analogy often used to describe the Internet aptly reminds us of the inherent decentralised and open architecture of the Internet (Lessig 2002). Although created originally for small and specialised communities operating in an environment of trust, the rapid global expansion of the Internet renders it highly vulnerable to a lawless frontier-style Internet culture. Technology is now driving cultural adaptations and providing an environment for criminal opportunities that can no longer be addressed by the technological ‘fix’. The traditional notion of information security with an emphasis on system and data protection no longer captures the scope of the risks and threats now unleashed by digital and wireless connectivity. The role of public and private law enforcement is crucial in curtailing criminal activity and ensuring the digital ‘highways’ are not lawless or hazardous but safe for all who wish to travel them. As digital technology becomes more pervasive

and interconnected, ordinary crime scenes will contain some form of digital evidence. Crucially many cyber crimes take place across jurisdictional boundaries with offenders routing attacks through various jurisdictions and can only be countered by a cross-border and international policing response.

As a result, the need for reliable and efficient mechanisms for international cooperation in law enforcement matters has never been more urgent. 'The fight against cyber-crime either is a global one or it makes no sense' (Esposito, 2004:54). As noted, the international community has taken a number of significant steps to facilitate cross-border cooperation in criminal matters, including in the investigation and prosecution of cyber-crime. This paper considers some of the avenues for cooperation. The focus is on the fast growing Asia Pacific region where the digital divide is extreme and the challenge of international cooperation consequently great. For certain, North Asia and China in particular will be super-weight players in any global system of cyber-crime prevention. However rapid the growth of information and communications technologies (ICT) may be, it is unlikely to continue its apparently exponential trajectory unless the digital divide is broken and poorer nations and neighbours are included. This is unlikely unless multinational corporations and governments in the richer states undertake positive long-term investment where it is most needed.

Criminality and Computer Crime

With government, industries, markets and consumers increasingly dependent on computer connectivity, they are prone to an array of threats. The most notable have been the widely publicised computer 'viruses', which have increased in both virulence and velocity since 2000. The beginning of 2004 saw the development of increasingly complex malicious code in the form of the "MyDoom" or "Norvag" worm. It apparently combined the effects of a worm, spreading rapidly across the Internet, with that of a distributed denial of service attack, where computing power is directed at a target system with a view towards shutting it down. In other words, infected computers were remotely 'commandeered' and directed against the target computer. The risks now posed by the release of malicious codes of increasing complexity (often specifically targeted against either a significant commercial or government site) were substantial and could threaten the viability of e-commerce (Moore et al. 2003, Staniford et al., 2002). Many observers note the danger of under-estimating the 'communities of cyber- criminals' now operating in the various 'chat rooms' that proliferate on the Internet. Examples of these sorts of 'crime rookeries' can be found in the Internet web-based 'businesses' that often operate out of Eastern Europe and Russia to supply the latest counterfeit credit cards. At these e-commerce sites 'batches' of cards may be purchased on line from 'trustworthy' but deviant businessmen.

What is computer crime

The scope of criminal activities and their social consequences can be summarised by a typology of computer-related crime that comprises the following: conventional crimes in which computers are instrumental to the offence, such as child pornography and intellectual property theft; attacks on computer networks; and conventional criminal

cases in which evidence exists in digital form. The kinds of criminality encompass the following (by no means exhaustive) list:

- Interference with lawful use of a computer: cyber-vandalism and terrorism; denial of service; insertion of viruses, worms and other malicious code.
- Dissemination of offensive materials: pornography/child pornography; on-line gaming/betting; racist content; treasonous or sacrilegious content.
- Threatening Communications: extortion; cyber-stalking.
- Forgery/counterfeiting: ID theft; IP offences; software, CD, DVD piracy; copyright breaches etc.
- Fraud: payment card fraud and e-funds transfer fraud; theft of Internet and telephone services; auction house and catalogue fraud; consumer fraud and direct sales (e.g. virtual 'snake oils'); on-line securities fraud; and
- Other: Illegal interception of communications; commercial/corporate espionage; communications in furtherance of criminal conspiracies; electronic money laundering.

Many of these risks appear to mimic traditional criminal exploitation, albeit often executed with unprecedented ease, speed and impact across jurisdictions and thus the appropriate response is guided by new technological disciplines. The tasks of identifying cyber-criminals and bringing them to justice pose formidable challenges to law enforcement agencies across the globe, and require a degree and timeliness of cooperation that has been until only recently regarded as difficult, if not impossible, to achieve. However, computer intrusion is now more likely a predicate to a more serious offence. Forensic computing and evidence preservation protocols are essential to effective investigation and prosecution, especially given the trans-border nature of evidence collection (Pollitt 2003; Chan 2001). In most cases it is unlikely that a computer expert will be available at the crime scene and the risks of contaminating the evidence are high. Consequently, as with other types of crime, the emphasis is on following the traditional chain-of-evidence rules and ensuring that command and control assigns the relevant expertise promptly to the task at hand. Frequently this will require drawing on expertise in the private sector or academia.

Leading crime prevention scholars Newman and Clarke (2003) provide a review of crime prevention in the e-commerce context. In the online 'situation' the theft of information and the manipulation of identity and trust are the key. In their approach crime is an *opportunity* that occurs when the following conditions combine in time and place: the presence of motivated and tempted offenders (offender pathology is not required), and attractive and tempting targets in the absence of effective guardians. When this situation arises crime will occur providing the offenders also have appropriate resources (i.e. social and technical capital) to undertake the crime. Consequently efforts to reduce online offences and e-commerce crime need to recognise these basic ingredients and the numerous pathways or opportunities for crime in the online rather than face-to-face environment. A crucial factor is how trust is acquired and maintained when merchants must be more intrusive about their (unseen) customers' identity and credit risk and the apparent ease in which trust is manipulated by fraudsters and others operating in the online situation. Of interest is Newman and Clarke's attention to the risks posed in the post-transaction phase (i.e. the delivery of goods or services ordered), a matter often overlooked in discussions of cyber-crime. They note that most measures designed to counter crime in the e-

commerce environment relied on either identifying potential offenders or shoring up 'guardianship' via information security, but seldom addressed the relationship between these and nature of attractive targets. Risk-aversive systems of e-commerce therefore needed to be far more integrated than conventional environments and required attention to what information security engineers like to call 'social engineering'.

Policing computer-related crime in the global village

The relative novelty of computer crime has meant that most policing agencies have only recently developed specific measures for recording them. The advent of computer-related criminal laws and associated prosecutions and the establishment of computer emergency response teams (CERTs) and dedicated technology crime units within policing agencies, coupled with the development of crime victim awareness and consumer advocacy, have prompted jurisdictions at the forefront of the digital revolution to begin recording the incidence of illegality in cyberspace. However, in many jurisdictions cyber-crimes, if reported, may be not be differentiated from other commercial crime, fraud reports or criminal damage statistics or other categories. Thus the extent of computer-related crimes, even when reported, remains unclear. Police statistics about reported crime often tell us more about the activities and priorities of police than they do about the extent of crime. This is because in many traditional crimes, victims do not report them to the authorities. This is undoubtedly also the case for computer crime.

The transnational nature of cyber-crime reflects the process of globalisation, which has intensified over the past two decades. The emergence of e-commerce, as well as the social dimension of the Internet and associated 'cyber-crimes', is a striking example of the challenges to the independent capability of nation-states to regulate social and economic order within their territories. Radical versions of globalisation go further and suggest that the nation-state system of international relations no longer provides an effective methodology for regulating either domestic or transnational activity, especially international trade. In either version of globalisation, 'sub-state' actors, such as large commercial institutions, play a crucial role in the emergence of what Sheptycki (2000) terms a transnational-state-system. In this system new configurations of actors and power emerge and transnational organisations (both licit and illicit) will flourish due to the diminishing sway of the state (Lizee 2000: 165). Given this context, what may eventuate in the absence of the rule of law in transnational environments is 'governance without governments' (Rosenau 1992). Shannon and Thomas (2005) also stress 'human security' perspectives in dealing with complex threats posed by cyber-crime and argue that over-reliance on the State, especially the public police, to address cyber-security issues would expose both markets and society to frequent low level but costly risks. Consequently the role of public-private police partnerships in the market-place and the emergence of civil society on the Internet combined with public awareness has become essential to contain cyber-crime amongst ordinary users.

While there now exist international conventions and treaties expressly designed to inhibit serious criminal networks or offenders operating across borders, the reach of these instruments is limited by the speed and scale of domestic ratification and consequential enabling laws. In dealing with IT crime, law enforcement is at a

disadvantage because of the remarkable speed in which cyber-crimes unfold against the typically 'low-speed cooperation' offered by traditional forms of mutual legal assistance. The role of multinational agencies such as Interpol and the United Nations has never been more essential. Yet within Asia (and globally) the results fall far short of creating a seamless web of bilateral or multilateral agreements and enforcement that would ensure a hostile environment for cyber criminals. The compatibility of criminal activity with these global changes is illustrated by the expansion and convergence of the profitable business of smuggling of humans, pornography, narcotics or other illicit commodities with the development of communication infrastructure and trade.

International Legal Cooperation

The passage of the Council of Europe's Cyber-crime Convention in December 2001 and its activation in July 2004 provides for the first time an international legal mechanism for cooperation in law enforcement and harmonisation of laws (see Csonka 2005, Esposito 2004, Tanabe 2004 and Cross 2003). Forty-two states have signed the Convention (including non-Council member states: Canada, South Africa, Japan and the United States) but as of 2005 only 11 states had ratified the convention. Nevertheless, given the cumbersome nature of treaty ascension processes the ratification and activation (a minimum of five ratifications are necessary) of this Convention in less than three years has been extraordinarily rapid. The Convention's 'First Additional Protocol to the Convention on Cybercrime on the criminalisation of acts of a racist or xenophobic nature committed through computer systems' that extends 'content' cybercrime to include 'hate speech' as well as child pornography has been signed by 25 states and awaits the ratification process (only 4 ratifications have occurred see http://conventions.coe.int/Treaty/; visited September 22, 2005). Apart from widespread global efforts to suppress child pornography (De Schrijver, Van Renterghem and De Pauw 2004) little progress outside of Europe may be expected in relation to the kinds of hate crimes captured by the additional protocol (Broadhurst, 2004).

The Convention, apart from enhancing mutual legal assistance (MLA), provides comprehensive powers to expedite preservation of stored computer data and partial disclosure of traffic data; to make production orders; to search computer systems; to seize stored computer data; to enable real-time collection of traffic data; and to intercept the content of questionable electronic data. A number of countries outside the Council of Europe, notably in South America are considering similar model legislation (see OAS recommendations on an inter-American cyber-crime instrument at http://www.oas.org/juridico/english/cyber.htm.) The convention is also open to any non-member state wishing to join (via a request to the Committee of Ministers of the Council of Europe). Indeed many jurisdictions in the Asian region, Thailand in particular, have looked at the Convention for guidance in formulating national laws. The hope was that the Council of Europe's treaty would be widely ratified (Esposito 2000:64). However, adoption of the Convention is not likely to be universal (Csonka 2005: 326). Given the pressing need for a broader multilateral structure for cross-border cooperation in the computer crime area, every effort should be made to open up the Convention for widespread accession as soon as is practicable (Bullwinkel 2005).

These developments are mirrored by the increasing transnational activities of corporate and private security. Indeed, given the role of (self-) regulatory approaches by corporations, especially multinational enterprises, the role for transnational private policing is already significant and widespread (Johnston 2000). For example, private security is the major provider in the payment card industry, intellectual property investigations and airline security. The sheer volume of potential global cyber-crime activity compels police partnerships with banks, telecommunication providers and corporations. Partnerships also raise real issues of shared intelligence in environments of trust. Thus the mobilisation of so-called 'private police' and non-government organisations in partnership with public police are essential if cyber-crime is to be contained. Crime exploits the 'gaps' in the sovereign state system of international relations and unless it is recognised that in communities of 'shared fate', coordinated forms of regulatory endeavour (free, for example, from unduly strict or pedantic definitions of 'dual criminality') may be the only means to curtail cyber-crime and its inevitable cross-border dimension.

United Nations Convention Against Transnational Organized Crime
Since the early 1990s, beginning with the Eighth United Nations (UN) Congress on the Prevention of Crime and the Treatment of Offenders (1990), the United Nations, with its network of institutes on crime prevention and criminal justice, has been actively involved in addressing problems of transnational crime and cyber-crime. The scope of computer-related crime affects every country in the UN and the UN General Assembly (GA) in 2001 promoted new international efforts to assist member states in dealing with computer-related crime. The Assembly in its 'Plans of action for the implementation of the Vienna Declaration on Crime and Justice: Meeting the Challenges of the Twenty-first Century' (GA resolution 56/261) devoted a special section to 'Action against high-technology and computer-related crime', in which it provided action-oriented policy recommendations for the prevention and control of these crimes. In 2002, the General Assembly addressed again the Vienna Plan of Action (GA resolution 57/170), and through the Commission on Crime Prevention and Criminal Justice recommended that the Eleventh United Congress on Crime Prevention and Criminal Justice (Bangkok, 18–25 April 2005) consider the plan. In 2001, the UN Secretary-General explored various options for further work on high-technology and computer-related crime including: whether a global 'treaty', if any, should be normative or legally binding; what relationship, if any, this would have to the UN Convention against Transnational Organised Crime; how a treaty, once concluded, could be kept up to date; and how it may accommodate issues such as privacy, freedom of expression and other human rights and commercial interests (Redo 2004; Bowman 1996). The Eleventh Congress, as noted deferred action on the development of a UN cyber-crime treaty.

Although not specifically directed at cyber-crime, the complementary role of the UN Convention Against Transnational Organized Crime (in force as of 2003) is a highly relevant global instrument for addressing some of the more nefarious aspects of cyber-crime. The UN Convention Against Transnational Organised Crime (the TOC Convention) was introduced in December 2000 in Palermo, Italy. The TOC Convention has been signed by 147 States (and 110 parties) and came into force on the 23 September 2003 (see www.undcp.org/crime_cicp_signatures_convention.html; visited September 22, 2005.) The TOC Convention significantly extends the reach of the 1988 Vienna Convention Against Illicit Traffic in Narcotics and Psychotropic

Substances. The TOC Convention enables mutual legal assistance (MLA) between states and establishes several offence categories: participation in an organised criminal group, money laundering, corruption and obstruction of justice as well as protocols in respect to trafficking in women and children (117 States and 64 parties with effect from December 25, 2003); illicit manufacturing and trafficking in firearms (52 States and 22 parties but not yet in force); and smuggling of migrants (112 States and 57 parties with effect 28 January 2004). Serious crime is defined broadly (conduct attracting punishment of four or more years' imprisonment). The basis of the framework is one that yields such flexibility in the definitions of both organised and transnational crime that it may serve as a generic legislative model across diverse common law and continental systems. In addition, the TOC Convention expressly refers (Article 29 (2)) to methods for combating the misuse of computers and telecommunications networks, provisions for training and materials, especially assistance for developing countries, and places obligations on capable states. The TOC Convention also establishes a number of principles and arrangements for international cooperation, which may be taken as an example of a potent global instrument against cyber-crime, in line with Article 13.1 (a) of the United Nations Charter emphasising the progressive development of international law. They include regulations limiting the rule of double criminality for mutual assistance purposes and introduce 'enterprise' responsibility.

The scope of the TOC Convention includes particular offences signatories are obliged to criminalise **(**Articles 5, 6, 8 and 23) as well as 'serious crime' (as defined in the Convention), 'where the offence is transnational in nature and involves an organized criminal group' (see Article 3(1)). Importantly, the definitions of 'serious crime' and 'organised criminal group' reflect an understanding that organised criminal activity is no longer confined to a relatively narrow range of offences traditionally associated with organisations such as Triads and the Cosa Nostra. The TOC Convention, defines an offence as 'transnational' if it is: (a) committed in more than one State; (b) committed in a single State but planned, prepared, directed or controlled in another State; (c) committed in one State but involving an organised group whose activities cross national boundaries; or (d) committed in a single State but has 'substantial effects' in another State (see Article 3(2)). Many of the most common forms of cyber-crime therefore qualify as 'serious crime' because such offences usually affect more than a single jurisdiction, often involve at least three or more actors, and are committed with the aim of achieving some financial or material benefit.

Article 27 deals with police-to-police cooperation and reflects the types of assistance routinely provided among police officials in the absence of a formal agreement and reflects international consensus on the need for close coordination between law enforcement authorities. To achieve this goal, States are encouraged to promote the exchange of personnel and other experts, including liaison officers. Additionally, signatories are required to 'make full use of agreements or arrangements, including international or regional organisations, to enhance the cooperation between their law enforcement agencies' (Article 27(2)). With respect to formal MLA, Article 18 contains provisions nearly as lengthy and detailed as a comprehensive bilateral MLA treaty. States may seek assistance in connection with: taking evidence or statements from persons; executing searches and seizures; obtaining business and/or government records; and identifying and tracing the proceeds of crime. A requested State has the discretion to decline assistance on the ground of the absence of dual criminality – a

potentially significant limitation in the cyber-crime context, as many countries do not have fully developed legislation in this area. The TOC Convention also provides for extradition (Article 16) even where a State Party makes extradition conditional on the existence of a bilateral treaty, Article 16 represents a major step forward because its effect is to incorporate into existing bilateral treaty relationships the numerous offences 'covered by' the Convention (Article 16(3)). Thus where two States Parties have relied on outdated and narrow extradition agreements (such as a list-based treaty providing for extradition only in relation to a specified list of offences), the TOC Convention will substantially expand the range of extraditable offences between them (Bullwinkel 2005; Cross 2003).

The Council of Europe Cyber-crime Convention

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. As one of the two principal supranational organisations in Europe (the other being the European Union), the CoE is responsible for creating and implementing a wide variety of measures aimed at international crime and has adopted a number of widely used conventions on interstate cooperation in penal matters. In 1996, the CoE's European Committee on Crime Problems established a committee of experts to address cyber-crime, which completed its work late in 2001.

The resulting Cyber-crime Convention has three aims: to lay down common definitions of certain criminal offences – nine are mentioned in the Convention – thus enabling relevant legislation to be harmonised at national level; to define common types of investigative powers better suited to the information technology environment, thus enabling criminal procedures to be brought into line between countries; and to determine both traditional and new types of international cooperation, thus enabling cooperating countries to rapidly implement the arrangements for investigation and prosecution advocated by the Convention in concert, for example by using a network of permanent contacts. The Convention, has received strong support from lawmakers and practitioners throughout Europe and beyond. But both the Convention and its Additional Protocol have been criticised on various grounds by a number of associations, particularly those active in the protection of freedom of expression, and also by industry elements (Csonka 2005).

The CoE Convention on Cyber-crime (the 'Convention') obligates signatories to criminalise a minimum list of specific offences where there was consensus and thus harmonised offences to eliminate problems of dual criminality. The basic structure and content of the convention is outlined below.

Computer related offences
Title 1 addresses offences against the confidentiality, integrity and availability of computer data such as: (1) illegal access of a computer system; (2) interception of non-public transmissions of computer data to, from, or within a computer system; (3) interference with computer data; (4) interference with computer systems, such as computer sabotage; and (5) the misuse of computer-related devices (e.g. 'hacker

tools'), including the production, sale, procurement for use, import or distribution of such devices. By criminalising illegal access, that is, 'hacking', 'cracking' or 'computer trespass', sends a clear signal that this conduct is illegal in itself and will be prosecuted: such intrusions may give access to confidential data (including passwords, information about the targeted system) and secrets or to 'free' use of the system and might encourage hackers to commit more dangerous forms of computer-related offences, like computer-related fraud or forgery. The criminalisation of illegal interception protects the privacy rights of data communication and seeks to deter the tapping and recording of communications between persons and applies this principle to all forms of electronic data transfer, whether by telephone, fax, e-mail or file transfer. The provision on data interference aims at providing computer data and computer programs with protection similar to that enjoyed by corporeal objects against intentional infliction of damage. Conduct, such as damaging, deteriorating or deleting computer data, reduces the integrity or content of data and programs also captures malicious codes, and viruses (e.g. Trojan horses).

The Convention criminalises acts of computer sabotage and covers the intentional hindering of the lawful use of computer systems, including telecommunications facilities, by using or influencing computer data (system interference). The section covering misuse of devices establishes a separate criminal offence including some specific conduct (production, distribution, sale, etc.) involving access devices, which were primarily designed or adapted for misuse. Devices that are designed and used for legal purposes are not included. This offence therefore requires a particular purpose, that is, committing any of the other offences against the confidentiality, integrity and availability of computer systems or data. Title 2 covers the traditional offences of fraud and forgery when carried out through a computer system. For forgery, the intent of this provision is to protect computer data in the same manner as tangible documents, where such data may be acted upon or used for legal purposes (Esposito 2004). Note, chapter 5 obliges signatories to criminalise the attempt to commit certain offences on which the Convention imposes a criminalisation obligation, as well as aiding and abetting the commission of offences and also provides for the liability of legal persons.

Content-related offences

Title 3 seeks to control the use of computer systems as a vehicle for the sexual exploitation of children and acts of racists or xenophobic nature. This category of offences concerns the subject or contents of computer communications and focuses on offences related to children. The Convention makes various acts (from the possession to the intentional distribution of child pornography) criminal offences, thus covering all links in the chain. This provision criminalises various aspects of the electronic production, possession and distribution of child pornography. Most states already criminalise the traditional production and physical distribution of child pornography, but with increasing use of the Internet as the main method to distribute such material specific provisions were essential to combat this new form of sexual exploitation of children. Other types of illegal content, such as racist propaganda, have also been included but in the form of an Additional Protocol criminalising racist propaganda. Esposito (2004) notes that cyber-crime is now defined as crimes committed against and through computer systems. The CoE's Cyber-crime Convention was originally intended to cover only the first category, while there is a growing consensus, at least in Europe, of the need to address the second category (e.g. Article 9 of the Cyber-

crime Convention on cyber-pedopornography, and the Additional Protocol on the fight against racism and xenophobia on the Internet).

Offences related to copyright infringement
Title 4 criminalises wilful infringements of copyright and related rights when such infringements have been committed by means of a computer system and on a commercial scale. This section targets the large-scale distribution of illegal copies of works protected by intellectual property rights (IPR). Infringements of IPR, in particular of copyright, are among the most commonly committed offences on the Internet, and cause concern both to copyright holders and those who work professionally with computer networks.

Jurisdiction
Among the various important matters addressed by the Convention, was the question of jurisdiction in relation to information technology offences, for example to determine the place where the offence was committed and which law should accordingly apply, including the case of multiple jurisdictions and the question of how to solve jurisdictional conflicts. This provision establishes criteria under which contracting parties are obliged to establish jurisdiction over the criminal offences in the Convention. The provision concerning jurisdiction also requires states exercising jurisdiction to coordinate when victims are located in different countries.

Procedural Powers
The procedural part of the Convention, which also applies to the Additional Protocol aims to enable the prosecution of computer crime by establishing common procedural rules and adapting traditional measures such as search and seizure and creating new measures, such as expedited preservation of data, to remain effective in the volatile technological environment. As data in the IT environment is dynamic, other evidence collection relevant to telecommunications (such as real-time collection of traffic data and interception of content data) has also been adapted to permit the collection of electronic data in the process of communication.

Despite fears to the contrary, the Convention addresses specific criminal investigations and does not set up an 'Orwellian' system of electronic surveillance (Esposito 2004). It enables data to be seized, or obliges those who possess the relevant data to disclose, or preserve data for investigation, but the Convention does not require or justify the surveillance of personal communications or contacts, by either service providers or police, unless there is an official criminal investigation. In addition, strong procedural guarantees are included. The Convention will be subject to the safeguards provided for by the domestic law of each party, and provides human rights protection, as defined by the relevant international instruments (in particular the European Commission on Human Rights and the International Covenant on Civil and Political Rights). It also advocates that before applying the Convention's powers states should ensure that these are proportional to the nature and circumstances of the offence under investigation.

The Convention 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 general scope of the obligation to cooperate stems

from the procedural powers defined by the treaty: cooperation is to be provided in relation to the offences established, as well as to criminal offences related to computer systems and data and to the collection of evidence in electronic form. Thus, if the crime is committed by use of a computer system, or where an ordinary crime not involving the use of a computer system occurs (e.g. murder) but involves electronic evidence, the Convention applies.

The Convention also creates the legal basis for an international computer crime assistance network, 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 hours a day, seven 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 provided by the Convention to ensure States can respond effectively to the law enforcement challenges posed by computer crime. This network will supplement the more traditional channels of cooperation. Each national 24/7 contact point is to either facilitate or directly carry out technical or legal advice, preservation of data, collection of evidence, and locating of suspects. The Convention also requires that national network team be properly trained to respond to computer-related crime.

The most intrusive powers in the Convention, as Csonka (2005) notes, are the *real-time collection of traffic data* and the *real-time interception of content data*. Both powers must be associated with specified communications transmitted by a computer system. Both powers enable the real-time collection or real-time interception of data by police or by service providers. With the convergence of telecommunication and information technologies, the distinction between telecommunications and computer communications is becoming blurred. Thus 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 data that can be ordered to be collected is of two types: the first concerns traffic data, the second content data. 'Traffic data' is defined as any computer data relating to a communication made by means of a computer system or generated by a computer system and which formed a part of the chain of communication, indicating the communication's origin, destination, path or route, time, date, size and duration or the type of service. 'Content data' is not defined in the Convention but refers to the substance of the communication, that is, the meaning of the communication, or the message or information being conveyed (other than traffic data).

Global and regional cooperation

Cyber-crime creates an unprecedented need for concerted action from government and industry, but also unprecedented challenges to effective international cooperation. As noted it is not always clear where computer-related offences take place for the purpose of determining criminal jurisdiction. An offence may produce victims in many countries, as in cases involving virus attacks, copyright violations, and other

offences carried out globally through the Internet. This in turn may result in cross-border conflicts regarding which jurisdiction(s) should prosecute the offender and how such prosecutions can be carried out to avoid inconvenience to witnesses, duplication of effort, and unnecessary competition among law enforcement officials (Bullwinkel 2005).

The various measures now operating within the European Union, the Council of Europe's Convention, the establishment of EUROPOL and a European Judicial Network, provide examples of greater law harmonisation and fewer opportunities for transnational criminals to exploit jurisdictional and legal loopholes between nations. European initiatives in international crime provide sound examples of the way forward in regional cooperation, but may not serve as a model for the development of countermeasures in the vastly different socio-cultural and economic circumstances found in Africa or Asia (Khoo 2003). Nonetheless, it is clear that cyber-crime, and not just the traditional concerns about narcotics and piracy are matters of significant concern. Thus 'international law enforcement' has shifted from a peripheral to a central role within otherwise domestically focused law enforcement agencies. In addition, the lines between the policing function and national security appear less distinct, and considerable overlap now routinely occurs between the agencies countering threats such as cyber-crime, low-intensity warfare and terrorism. Thus importance is attached to intra-agency cooperation within jurisdictions and the need to improve and maintain these in order to enhance MLA at the regional and international level.

Regional efforts outside of Europe are also underway via OAS, ASEAN and the APEC forum. Such developments have yet to evolve into fully institutionalised forms of cross-border legal cooperation or to determine the response of states within the region. There are now significant regional forums for police and other law enforcement officials and there is routine exchange of consular police liaison officers (Aiziwa 2001). The leading organisations, apart from the United Nations and the Council of Europe already described, involved in developing international and regional efforts against cyber-crime are briefly described in the sections to follow.

G8 Senior Experts Group on Transnational Organised Crime
The Group of Eight (comprising Canada, Germany, France, Italy, Japan, the United Kingdom, United States and since 1995 - Russia) although originally established to co-ordinate economic policy has as well developed initiatives to combat international crime. At the Halifax Summit in 1995, G8 heads of state established a cross-disciplinary group of senior government experts (the 'Lyon Group') to address methods of combating transnational organised crime. In 1996 the Lyon Group devised 40 recommendations aimed at increasing the efficiency of collective action against transnational organised crime via two interrelated goals: strengthened capacity in the investigation and prosecution of high-tech crime; and more effective regimes for cross-border cooperation in criminal matters.

The Forty Recommendations cover a range of issues and emphasised the need to eliminate delay in respect to traditional forms of cross-border assistance (such as informal police cooperation, mutual legal assistance, and extradition), and a coordinated approach in tackling high-tech crime. As a consequence of these recommendations the Lyon Group's 'High-Tech Crime Subgroup' was established

and quickly thereafter the 24/7 computer security network which has now expanded to countries outside the G8. As of the end 2004, 40 countries participate in the global 24/7 network. Later G8 ministers endorsed a set of principles and an action plan to respond to transnational cyber-crime cases that included; provision of adequate personnel and training to fight high-tech crime; domestic laws that criminalised cyber-crime and ensure that relevant evidence, including traffic data, could be preserved and obtained expeditiously; and coordination with industry to ensure that new technologies are developed in a way that will facilitate law enforcement action against cyber-criminals. The 1999 Moscow meeting later endorsed principles on trans-border access to stored computer data and called for a comprehensive response to Internet fraud and more industry coordination. A joint communiqué of the G8 Home Affairs Ministers meeting in Washington on May 10, 2004 noted, given the activation of the Council of Europe's Convention on Cybercrime, that action was required "…to encourage the adoption of the legal standards it contains on a broad basis" and, "…all countries must continue to improve laws that criminalize misuses of computer networks and that allow for faster cooperation on Internet-related investigations" (see http://www.g7.utoronto.ca/justice/justice040511_comm.htm visited November 14, 2004*).*

ASEAN

ASEAN comprises 10 nations: Brunei Darussalam, Cambodia, Indonesia, Laos, Malaysia, Philippines, Singapore, Thailand, Myanmar and, Vietnam. While ASEAN has provided a limited pan-Asian approach, it does form a basis for developing a wider regional forum for considering matters of MLA. Its approach, even given the developing nature of the region, mirrors the methodology of the European Union. The sheer cultural and economic diversity of Asia makes the process of multilateralism fraught with difficulty (Khoo 2003). Yet understanding the different capacities and perspectives of how each state could contribute was an essential first step. The endorsement in October 2000 of the action plan of the ASEAN and China Cooperative Operations in Response to Dangerous Drugs (ACCORD) in partnership with the United Nations Drug Control Program (UNDCP) illustrates the quickening of MLA responses to transnational crime such as cyber-crime. ASEAN has conducted four ministerial meetings on problems of transnational crime (Manila 1997, Yangon 1999, Singapore 2001, Bangkok 2003). These meetings oversee the work of the Annual Senior Officials Meeting on Transnational Crime and consider the deliberations of meetings of the ASEAN National Chiefs of Police (ASEANAPOL) and their cooperative efforts to combat transnational crime.

In 1997, ASEAN interior and home affairs ministers gathered in Manila for the First ASEAN Conference on Transnational Crime and issued a declaration outlining a variety of measures aimed at enhancing regional coordination and cooperation in criminal matters. If fully implemented and adequately resourced, the proposals would represent a substantial advance in regional law enforcement cooperation. ASEAN ministers agreed to: biannual ministerial meetings to coordinate the activities of relevant bodies such as the ASEAN chiefs of national police (ASEANAPOL); hold discussions with a view to signing MLA treaties, other bilateral treaties and memoranda of understanding among ASEAN member countries; establish an ASEAN Centre on Transnational Crime with the task of coordinating regional efforts against international crime through intelligence-sharing, harmonisation of policies and

operational coordination; convene a high-level ad hoc experts group tasked with developing an action plan for tackling transnational crime and an institutional framework for regional cooperation; and encourage members to facilitate cooperation among law enforcement by posting of foreign liaison officers (see ASEAN Declaration on Transnational Crime, signed on December 20, 1997 in Manila: available at http://www.aseansec.org/politics/adtc97.htm; visited, November 21, 2003). At the Second ASEAN Ministerial Meeting on Transnational Crime (held in Myanmar in 1999), ASEAN ministers issued another ambitious communiqué outlining a broad plan of action to enhance collective efforts against the many forms of organised criminality in the region. A group of senior government officials (referred to as the Senior Officials Meeting on Transnational Crime or SOMTC) has been tasked to assist in the execution of ministerial initiatives and directives.

The theme of greater cooperation carried over to the Third and Fourth ASEAN Ministerial Meeting on Transnational Crime, at which ASEAN ministers reiterated their commitment to collaborate further in the battle against computer-related crime and called for a stronger partnership between ASEAN and other partners and agencies, including Interpol and the United Nations (see Joint Communique of the Third ASEAN Ministerial Meeting on Transnational Crime issued on October 11, 2001 in Singapore: available at http://www.aseansec.or.id/5621.htm, visited November 21, 2003). As noted, the ASEAN anti-crime institutions, particularly SOMTC, mimics the G8's Lyon Group, indicating the relevance of such frameworks for collective government action. Particularly significant is that ASEAN's law enforcement experts group reports directly to ministers and thus, like the G8's Lyon Group, has the capacity to develop policies with support at the highest levels.

The European Union and Europol

The 1957 Treaty of Rome established the European Economic Community, which in turn evolved into the European Union (EU), established under the Treaty of Maastricht in 1992. The EU has 28 member States and recently completed the accession of 13 countries in eastern and southern Europe (with some new members joining on 1 May 2004). It includes supranational institutions that address international crime by adopting joint positions, directives and other instruments addressing a wide variety of criminal activities. Among the most important in respect to the coordination of law enforcement are: the adoption of a common position on negotiations relating to the CoE Cyber-crime Convention and EU conventions on mutual assistance in criminal matters and extradition (see http://www.europa.eu.int/scadplus/leg/en/lvb/114015b.htm; visited December 11, 2003), the establishment of a 'European Judicial Network,' consisting of liaison magistrates and representatives responsible for international judicial cooperation, and tasked with facilitating cross-border cooperation (see http://www.europa.eu.int/scadplus/leg/en/lvb/133055.htm; visited December 11, 2003). Further strengthening of MLA is contained in the April 19, 2002 'Proposal for a Council Framework Decision on Attacks Against Information Systems'.

Included within the EU is the European Police Office or Europol, dedicated to increasing the efficiency of cooperation among the police agencies of EU member states, with an emphasis on targeting organised crime. Based in Brussels, Europol is accountable to the EU's Council of Ministers for Justice and Home Affairs. The organisation is comprised of European Liaison Officers (who represent national law

enforcement agencies across the EU, including police, customs, and immigration officials), and Europol staff officers. Like Interpol, Europol's primary function is to support the operational activities of national law enforcement officials and recently extended to include the fight against cyber-crime. In furtherance of this its representatives facilitate the exchange of information, provide analyses of criminal intelligence, generate strategic reports on trends and patterns of criminal activity, and provide technical expertise for ongoing investigations within the EU. In addition, it is likely Europol will eventually assume a greater investigative and operational role.

The Organisation for Economic and Cultural Development (OECD)
Established in Paris in 1960 by 20 countries (now 30 members) the OECD aims to promote economic and social welfare throughout the OECD by helping member states to coordinate their efforts to aid less developed nations. The OECD has established a presence in law enforcement, for example, by establishing a Bribery Working Group, whose efforts ultimately led to the adoption of a convention against commercial bribery. The OECD has been active in the area of cyber-crime and online security especially in regard to encryption technology, evaluating the balance between law enforcement and privacy concerns and the means by which member states can coordinate encryption policy, and in 1997 issued a series of guidelines addressing these issues. More recently, in the wake of the terrorist attacks of 11 September 2001, OECD governments developed a series of guidelines designed to counter cyber-terrorism, computer viruses, 'hacking' and related threats (see OECD Press Release dated August 7, 2002; available at http://www.oecd.org/EN/document/0,,EN-document-29-nodirectorate-no-12-33186-29,00.html). Although the recommendations are not legally binding, they reflect consensus among key jurisdictions on issues affecting the security of the online environment.

A highly effective approach to inter-governmental law enforcement coordination that offers a template for transnational cooperation against cyber-crime is the Financial Action Task Force (FATF) established at the G7 Paris Summit in 1989 and based in the OECD. FATF is a policymaking body whose aim is the implementation of legislative and regulatory reforms needed to combat money laundering. In 1990, the FATF issued a series of 40 recommendations addressing ways to combat and deter money laundering. The recommendations are grouped into three broad categories (criminal law, banking law and international cooperation) and serve as the basis for its activities. As a result of awareness-raising activities undertaken by FATF, a number of FATF-style organisations have also developed at the regional level including the Asian-Pacific region, the Asia/Pacific Group on Money Laundering (APG), established in 1997, operates in a manner similar to FATF and, in 2000 began to undertake a FATF-style mutual evaluation. A novel feature of FATF is that members are subject to peer review, a two-part process by which the group assesses implementation of the 40 recommendations. First, each FATF member conducts an annual self-assessment, using a standard questionnaire. Second, periodically members are subject to a process of mutual evaluation, involving a site visit by three or four experts from other member governments. Mutual evaluation has proved effective in persuading governments to take steps to fill gaps in anti-money laundering (see generally http://www.oecd.org/fatf/AboutFATF_en.htm).

Interpol

The International Criminal Police Organisation, or Interpol, consists of 181 member states. Headquartered in Lyon, France, Interpol coordinates its activities through National Central Bureaus in individual countries. Its mission, is to support law enforcement organisations throughout the world, in particular by facilitating the exchange of information, coordinating joint operational activities of member states, and developing and sharing expertise and best practices covering a wide range of criminal offences (see generally http://www.interpol.int/Public/icpo/Guide). Nearly half of Interpol's member countries lack the infrastructure for online communication (Noble 2003) and thus in respect to IT crime, Interpol has recognised the need for law enforcement officials to acquire specialised knowledge and has developed international training courses and manuals providing useful guidance for investigators working on computer-related crime (see http://www.interpol.int/Public/TechnologyCrime/WorkingParties/Default.asp#steeringCom).

Interpol's General Secretariat has also supported the formation of regionally organised working groups comprising local experts in computer-related crime who meet periodically to share experiences and develop best practices (Noble 2003). The Asia-South Pacific Working Party on Information Technology Crime currently meets annually, and has undertaken projects relating to the handling of digital evidence, forensic tools, and training. Interpol has also endeavoured to build close ties to existing regional structures in Asia, including ASEANAPOL, in an effort to build on regional cooperation by facilitating the development of regional intelligence databases and the wide dissemination of data through Interpol's extensive telecommunications network. Interpol has also stressed financial and high-technology crime as two of Interpol's top five priorities (along with drugs, terrorism, people smuggling and organised crime). Interpol has also increased its focus on intellectual property-related crime, because sophisticated and well-financed organised criminal groups increasingly carry out these offences on a global scale. Interpol hosted an initial meeting of its Intellectual Property Crime Action Group in July 2002 (see generally http://www.interpol.int/Public/FinancialCrime/IntellectualProperty/Default/.asp).

Generic problems of forgery and counterfeiting were the focus of Interpol's exemplary efforts in establishing a Universal Classification System for Counterfeit Payment Cards secure website. This secure site provides up-to-date information on trends and techniques with respect to the forgery of payment cards and fraud and enables law enforcement officials around the world to retrieve forensic data as well as general intelligence. Payment card industry representatives working in the anti-fraud area will also have access to the otherwise closed system. Apart from illustrating how Interpol's unique clearing-house function can be adapted to meet new problems, it showed that with support from the payment card industry the law enforcement community can better respond. As well as serving as an example of how international agencies can assist with essential tasks, such as secure shared intelligence it also exemplifies the role of private non-state actors in the prevention of crime.

Newton (2004) described how the Interpol Payment Card Website is also used to proactively inform law enforcement and payment card investigators about criminal conspiracies and, more importantly, to link apparently unconnected investigations in different countries and regions. He cites an example of an apparently isolated attack on an ATM in Toronto in 2002 by criminals using a false touch-sensitive PIN pad

device to compromise PINs and the electronic data contained on the magnetic stripes of genuine payment cards. The device covered the legitimate card slot on the ATM, and once customers' cards had been compromised a screen message advised customers to try again later. No transactions actually took place and consequently, in the absence of a seized device, it was difficult to identify the point of compromise. On this occasion the device was seized although the identity of the suspect(s) was unknown. Investigators in Toronto believed that the criminals responsible for the attack were situated in Eastern Europe. The case was publicised on the secure Payment Card website and as a result a further 11 attacks using identical devices were identified in Canada, Chile, Colombia and the United States. The other attacks revealed that the criminals were becoming more sophisticated; they were using transmitters to transmit compromised data to another location, thereby reducing the evidential value of seized devices. More importantly, it was eventually established that the perpetrators were actually an organised gang of Venezuelan criminals and not from Eastern Europe.

The intelligence was disseminated to investigators worldwide together with a warning that this criminal method was likely to migrate to other Spanish-speaking countries in the near future. In May 2003 two Venezuelan criminals were arrested in Seville carrying out identical attacks on ATMs in the city and another city in Spain. Several weeks later seven Venezuelans were arrested using the method in Portugal. Although Interpol does not claim direct responsibility for these arrests it is clear that with the close cooperation of NCR (a large manufacturer of ATMs), and more significantly users of the Payment Card website, it was possible to link these cases together and ensure that the law-enforcement and payment card community were fully aware of the extent of the criminal methods. Collectively they were able to respond more effectively to the threat posed by a determined and sophisticated group of international criminals.

Asia Pacific Economic Council (APEC)
Founded in 1989 in Canberra, for the purpose of promoting economic growth among member states, APEC now consists of 21 members. APEC is a consensus body that meets annually at the ministerial level and historically has focused on trade, but increasingly its members look to it as a vehicle for cross-border police cooperation. APEC's work over the past several years has also evolved (as with the G8 and OECD) a number of areas relevant to cyber-crime enforcement, including an Intellectual Property Rights Working Group (IPEG), and an Electronic Commerce Steering Group (ECSG -see generally http://www.apecsec.org.sg/workgroup/e-commerce.html). The objective of the ECSG, established in 1999, is to coordinate APEC-related activities in the area of e-commerce. Thus far, the ECSG has not directly addressed law enforcement issues in an e-commerce environment, but enforcement also connects to APEC's general interest in improving consumer trust and confidence in e-commerce. Further, the ECSG's increasingly detailed work in the areas of privacy and security in the online environment involve law enforcement concerns.

At their meeting in Los Cabos, Mexico, in October 2002, APEC leaders noted the threat of global terrorism and the importance of increasing the protection of global infrastructures and that global communications are only as secure as its weakest link, and collectively committed to: enact comprehensive cyber-security laws, on a par

with existing international standards, particularly the CoE Cyber-crime Convention and UN General Assembly Resolution 55/63 of 2000; identify or create national cyber-crime units and international high-technology assistance contact points; and establish computer emergency response teams, that exchange threat and vulnerability assessments and information. They also called for closer cooperation between law enforcement officials and businesses in the field of information security and fighting computer crime by endorsing the APEC Cyber-security Strategy. The elements of the strategy cover: legal developments; information sharing and cooperation; security and technical guidelines; public awareness; training and education; and wireless security. APEC's Telecommunications and Infrastructure Working Group has been most active in sponsoring projects to increase the ability of APEC member economies to more effectively address cyber-crime, including through greater intergovernmental and public–private sector cooperation (see http://www.apectelwg.org/apecdata/telwg/28tel/estg/telwg28-ESTG-09.htm).

Urbas (2005) observed in concluding an overview of legislation in Asia that the development of legislation designed to counter intellectual property offences and cyber-crime showed that while some states had enacted new laws, many remained ill-equipped to deal with the cross-border nature of these offences. Orlowski (2004) also reported an APEC cyber-crime legislation survey involving 14 nations that found all had some legislative provisions to address cyber-crime and to support law enforcement (see http://www.apectel28.com.tw/document/webword/estg/telwg28-ESTG-07.doc). However, mutual legal assistance, extradition arrangements, and provision of cross-border information in respect of computer offences were found in only half the countries surveyed. The survey noted that the main concerns related to the difficulties in requesting the collection and preservation of evidence in real time, issues relating to jurisdiction for offences and offenders, and lack of, or limitations in, mutual assistance and extradition arrangements. APEC has called for further work to develop laws and procedures that facilitate the investigation and prosecution of cross-jurisdictional cyber-crime. As noted above, it is essential to continually monitor progress and where necessary provide assistance and encouragement to ensure that MLA is not impeded.

Summary of measures for regional co-operation
Given the diversity of the above activities aimed at improving regional and international cooperation the basic ingredients for a global approach can be deduced. Grabosky and Broadhurst (2005) outline the basic elements of an effective regime for regional cooperation in combating cyber-crime that include the following:

- improve security awareness by providing adequate resources to secure transactions and equip system operators and administrators;
- improve coordination and collaboration by enabling systematic exchanges between the private sector and law enforcement including joint operations;
- take steps to ensure that technology does not outpace the ability of law enforcement to investigate and enact substantive and procedural laws adequate to cope with current and anticipated manifestations of cyber-crime;
- broadly criminalise the conduct (including juvenile offenders) and focus on all violators big and small;
- strengthen international initiatives by updating existing treaties and agreements to recognise the existence, threats and transnational nature of high-

tech computer-related crimes and strive for legal harmonization; and
- the development of forensic computing skills by law enforcement and investigative personnel and mechanisms for operational cooperation between law enforcement agencies from different countries, i.e. 24/7 points of contact for investigators.

Work-in-progress: comity between states and cyber-crime

In future, organised crime may be expected to recruit IT specialists, intimidate corporate insiders to obtain access to IT systems, and use anonymisers and encryption in furtherance of cyber-crime. In addition, there is evidence of the deployment of intelligent malicious software designed to elude detection by anti-virus software. Now automated 'intelligent' computer and network attack capabilities allow remote initiation of attacks to be directed at any computer or network on the Internet while making it more difficult to identify the actual source of the attack. These advanced forms of intrusion code enable users to gain competitive advantage by extracting sensitive economic data from competitors, provide data (such as customer's records) for extortion and denial of service offences. Most significantly, attacks are instantaneous and often remote, disregarding national sovereignty. Whether they are the work of a 14-year-old, a terrorist, a foreign intelligence service or an organised criminal may not be immediately apparent; all must be investigated. However, digital technology also affords new opportunities for individual citizens to communicate efficiently with police. An example is the Internet Fraud Complaint Center, which operates in the United States and receives on-line information from members of the public relating to questionable on-line activity and these are evaluated and referred to the appropriate agency or jurisdiction.

Digital footprints are fragile or ephemeral, so swift action is often required. This becomes very difficult when an attack transits multiple jurisdictions with different regimes for preserving evidence. Traditional methods of law enforcement are therefore no longer adequate. A slow formal process risks losing evidence, and multiple countries may be implicated. Following and preserving a chain of evidence is a great challenge. Among the challenges faced by investigators is the enormous increase in storage capacity in today's computers, and the challenge to effective and efficient searches that this entails. Almost every case will soon require computer forensics, and evidence will be located in multiple places. The challenge faced by investigators will be one of *information management* (Pollitt 2003). Even 'local' crimes may have an international dimension, and assistance may be required from all countries through which an attack was routed. An example is the case of 'Mafiaboy', whose distributed denial of service attacks in February 2000 was a watershed event: the seriousness of the threat and the vulnerability of e-commerce became apparent. The investigation of 'Mafiaboy' was a textbook example of close cooperation between the FBI and the Royal Canadian Mounted Police; only rapid and close collaboration between the two police services could have achieved such a result.

Many nations and regional bodies such as the Council of Europe have addressed the problem of cyber-crime and laws exist that criminalise unauthorised access and unlawful use of computers, but such laws are neither universal nor uniform. Concerns remain focused on the 'weakest links' in the supposedly seamless security chain necessary to prevent cyber-crime by predatory criminal groups. Comity thus can only

be assured if wealthy states and affected industries are prepared to extend aid to those states or agencies less capable. Consensus is the best strategy, for the suppression of computer-related crime entails a mixture of law enforcement, technological and market-based solutions. It can be argued, however, that a strict enforcement agenda is usually not feasible because of the limited capacity of the state. It is also feared that over-regulation could stifle commercial and technological development. Those sceptical of a heavily interventionist approach also argue that the marketplace may at times be able to provide more efficient solutions to the problems of computer-related crime than the state. Even if they were increased, police resources could never be enough. Deficits characterise the technical and computing capacities of public police, and it is often difficult to retain trained agents.

Although there is consensus about the risks of computer-related crime, apart from criminalising the conduct at a global level, there is much less consensus about what might be done to prevent it. There is concern that the technological solution to information security is a mirage, more hope than reality, and that dependence on the promise of a technology fix is an approach fated to fail. So also is the faith in a deterrence-based approach where the criminal law is deployed as the principal instrument of prevention. Deterrence is unlikely to succeed in all or even some circumstances, and experience with conventional crime suggests that over-reliance on the law, as a deterrent or moral educator alone is unlikely to help substantially even if legitimately supported by the community.

Fundamentally systems can be designed to lessen their vulnerability to criminal exploitation. Cyber-crime is often facilitated by vulnerable software, much of which is designed with user-friendliness and convenience in mind rather than security. The common industry response is for manufacturers to structure their licence conditions to avoid potential liability, then to make ‘patches’ available as vulnerabilities become apparent later on. Whether market forces will eventually drive the widespread development of truly secure software remains to be seen. Commercial enterprises may be in a position to achieve more protection than poorly resourced law enforcement agencies could deliver. In this respect I am reminded of earlier examples from the heyday of the mass production of the motor vehicle when consumer safety was knowingly compromised in the pursuit of profit. Manufacturers who quickly recognised the market value of safe products and retooled accordingly retained profitability, while those that did not faltered. Microsoft Corporation has now, it seems, reflected on its failure to lead the market in respect to consumer safety and to recognise that today the market demands a secure and trusted environment if computers and information technology are to realise their full potential.

References

Aizawa, K. 2001, 'Current mechanisms for International Cooperation in Criminal Matters: Mutual Legal Assistance and Extradition, 24/7 Points of Contact Network, and Training in the Field of Computer Crime', in Broadhurst, R. Ed, *Proceedings of the Asia Cyber Crime Summit*, Centre for Criminology: University of Hong Kong.

Bowman, M.E. 1996, 'Is international law ready for the information age?', *Fordham International Law Journal*, Vol. 19.

Bullwinkel, J. 2005, 'International Cooperation in Combating Cyber-Crime in Asia: Existing Mechanisms and New approaches', in R. Broadhurst and P. Grabosky, eds. *Cyber-Crime: The Challenge in Asia*, University of Hong Press.

Broadhurst, R.G. 2004, 'Content Cyber-Crimes: Criminality and Censorship in Asia', paper presented at the Council of Europe, Octopus Interface Conference on The Challenge of Cyber-Crime, Strasbourg, 15–17 September 2004.

Chan, H. 2001, 'Computer Forensics: A New Challenge to Crime Investigation', in Broadhurst, R. Ed, *Proceedings of the Asia Cyber Crime Summit*, Centre for Criminology: University of Hong Kong.

Council for Security Cooperation Asia and Pacific, 2004, 'Cybercrime and its Effects on the Asia Pacific Region: Report of the Transnational Crime Working Group', August 4, at http//www.police.govt.nz/events/2001/e-crime-forum/cybercrime_and_its_effects.html.

Csonka, P. 2005, 'The council of Europe Convention on Cybercrime: A Response to the challenge of the New Age?', in R. Broadhurst and P. Grabosky, eds. *Cyber-Crime: The Challenge in Asia*, University of Hong Press.

Cross, I. 2003, 'Enforcement and Prosecution Strategies in the 21st Century: Combating Multi-jurisdictional Crime', in R. Broadhurst (Ed.) *Bridging the GAP: A Global alliance on Transnational Organised Crime*, Hong Kong Police: Printing Department HKSAR.

De Schrijver, I., Van Renterghem, T., and H. De Pauw, 2004, 'Child Pornography on the Internet', paper presented at the Council of Europe, Octopus Interface Conference on The Challenge of Cyber-Crime, Strasbourg, 15–17 September 2004.

Esposito, G. 2004 'The Council of Europe Convention on Cyber-crime: A Revolutionary Instrument?', in Broadhurst, R. Ed, *Proceedings of the 2nd Asia Cyber Crime Summit*, Centre for Criminology: University of Hong Kong.

Grabosky, P. and R. Broadhurst 2005, 'The Future of Cyber-Crime in Asia', in R. Broadhurst and P. Grabosky, eds. *Cyber-Crime: The Challenge in Asia*, University of Hong Press.

Gros, J. 2003, 'Trouble in Paradise: Crime and Collapsed States in the Age of Globalization', *British Journal of Criminology*, 43: 63-80.

Khoo, B. H. 2003, 'Police Cooperation in Fighting Transnational Organised Crime: An Asian Perspective', in R. Broadhurst (Ed.) *Bridging the GAP: A Global alliance on Transnational Organised Crime,* Hong Kong Police: Printing Department HKSAR.

Korean Institute of Criminology, 2005, 'Workshop 6 'Measures to Combat Computer-related Crime', 11th UN Congress on Crime Prevention, Bangkok, April 22-23, 2005 with UN Office Drugs and Crime.

Iden, R. L. 2003, 'Cyber Crime: What's the Threat, the Challenge, and the Policing Response', in R. Broadhurst (Ed.) *Bridging the GAP: A Global alliance on Transnational Organised Crime,* Hong Kong Police: Printing Department HKSAR.

INCB 2001, Report of the International Narcotic Control Board 2001, UN E/INCB/2001/1.

Johnston L. 2000, 'Transnational private policing: the impact of global commercial security', in Sheptycki, J.W.E., Ed. 2000, *Issues in Transnational Policing,* Routledge: London.

Lessig, Lawrence 2002, *The Future of Ideas: the fate of the commons in a connected world,* Vintage, New York.

Levi, M. and D. Wall, 2004, 'Technologies, Security, and Privacy in the Post –9/11 European Information Society', *Journal of Law and Society*, 31:194-220.

Lisker, J. S. 2001, 'Electronic Commerce Fraud: Risk Assessment and Prevention', in Broadhurst, R. Ed, *Proceedings of the Asia Cyber Crime Summit,* Centre for Criminology: University of Hong Kong.

Lizee, P.P. 2000, *Peace, Power and Resistance in Cambodia: Global Governance and the Failure of International Conflict Resolution,* Macmillan: Houndsmill

Moore, D., Shannon, C. Voelker, G. M. and S. Savage, 2003, 'Internet Quarantine: Requirements for containing self-propagating code', IEEE INFOCOM

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

Newton, J. 2004, ' Interpol and the Cards Industry: Global Partnerships to Deliver Local Solutions', in Broadhurst, R. Ed, *Proceedings of the 2nd Asia Cyber Crime Summit,* Centre for Criminology: University of Hong Kong.

Noble, R. 2003, 'Interpol's New Approach: A Return to Basics', in R. Broadhurst (Ed.) *Bridging the GAP: A Global alliance on Transnational Organised Crime,* Hong Kong Police: Printing Department HKSAR.

Norris, P. 2001, *The Digital Divide: Civic Engagement, Information Poverty and the Internet Worldwide*. Cambridge University Press.

Orlowski, S. 2004, 'APEC Activities to Address Cybercrime Through Public/Private Cooperation', in Broadhurst, R. Ed, *Proceedings of the 2nd Asia Cyber Crime Summit*, Centre for Criminology: University of Hong Kong.

Pollitt, M. 2003, 'Digital Evidence in Internet Time', in R. Broadhurst (Ed.) *Bridging the GAP: A Global alliance on Transnational Organised Crime*, Hong Kong Police: Printing Department HKSAR.

United Nations, 2003, 'World Public Sector Report 2003, E-government at the Crossroads', Sales No. E.03.II.H.3, New York.

Urbas, G. 2005, 'Cyber-Crime Legislation in the Asia-Pacific Region', in R. Broadhurst and P. Grabosky, eds. *Cyber-Crime: The Challenge in Asia*, University of Hong Press.

Redo, S. 2004, 'The UN in Broadhurst, R. Ed, *Proceedings of the 2nd Asia Cyber Crime Summit*, Centre for Criminology: University of Hong Kong

Redo, S. 2000, 'Crime as the growing international security threat: the United Nations and effective countermeasures against transnational economic and computer crime', UNAFEI Resource Material Series No. 55, Tokyo, Fuchu, Japan, pp. 117–39.

Rosenau, J. N. 1992, 'The relocation of authority in a shrinking world', *Comparative Politics*, 24:253-72.

Sato, T. 2004, 'Countermeasures against Cyber-crime in Japan', in Broadhurst, R. Ed, *Proceedings of the 2nd Asia Cyber Crime Summit*, Centre for Criminology: University of Hong Kong.

Semple, K. 2004, 'E-Mail Worm Snarls Computers Around Globe'. *The New York Times Online*, 27 January http://www.nytimes.com/2004/01/27/technology/27CND-VIRU.html (visited 28 January 2004).

Shannon, J. and N. Thomas, 2005, 'Human Security and Cyber-Security: Operationalising a Policy Framework', in R. Broadhurst and P. Grabosky, eds. *Cyber-Crime: The Challenge in Asia*, University of Hong Press.

Sheptycki, J.W.E., Ed. 2000, *Issues in Transnational Policing*, Routledge: London.

Staniford, S, Paxson, V. and N. Weaver 2002, 'How to own the internet in your spare time', in Proceedings of the 11th USENIX Security Symposium (Security '02), available at http//www.icir.org/vern/papers/cdc-usenix-sec02/, visited December 9, 2003.

Sussmann, M.A. 1999, 'The Critical Challenges from International High-Tech and Computer-Related Crime at the Millennium', *Duke J. of Comp. & Int'l L.*, 9:451

Tanabe, Y., 2004, 'Inter-governmental Cooperation in Combating Cybercrime – UN Workshop on Crime Related to Computer Networks', in Broadhurst, R. Ed,

Proceedings of the 2nd Asia Cyber Crime Summit, Centre for Criminology: University of Hong Kong.