Combating the Cybercrime Threat: Developments in Global Law Enforcement

Roderic Broadhurst, *Queensland University of Technology*

Introduction 210
Criminality and Computer Crime 211
What Is Computer Crime? 211
Transnational Policing and Cybercrime 212
United Nations Convention against Transnational Organized Crime 213
The Council of Europe Cybercrime Convention 214
Computer-Related Offenses 214
Content-Related Offenses 215
Offenses Related to Copyright Infringement 215
Jurisdiction 215
Procedural Powers 215
Global and Regional Cooperation 215
G8 Senior Experts Group on Transnational Organized Crime 216
ASEAN 216
The European Union and Europol 217
The Organization for Economic Cooperation and Development 217
Interpol 218
APEC 218
Summary of Measures for Regional Cooperation 219
Glossary 220
Cross References 220
References 220

INTRODUCTION

The rapid development of computer connectivity and the role of the Internet in the emergence of new e-commerce markets are key generators of the processes of globalization and 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. Although the process of globalization 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 have been reactive rather than proactive.

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. The new opportunities created in cyberspace have also enhanced the capacity for criminal enterprises to operate more efficiently and effectively both domestically and across borders. Law enforcement agencies in many jurisdictions have been unable to respond effectively and even in the most advanced nations, 'play catch-up' with cybersavvy criminals (Sussmann, 1999). 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. 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. The basic issue of how to police this new arena, cyberspace, is the focus in this chapter (for related discussion of cybersecurity systems for military purposes or asymmetric warfare see chapters "Online Stalking," "Wireless Information Warfare," and "Information Assurance").

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. At the international level, two new treaty instruments provide a sound basis for the essential cross-border law enforcement cooperation required to combat cybercrime and are briefly discussed. The first is the purpose-built Council of Europe's (CoE) Cybercrime Convention, which, although it was designed as a regional mechanism, has global significance. The second is the United Nations Convention against Transnational Organized Crime (TOC Convention), which is global in scope but indirectly deals with cybercrime when carried out by criminal networks in relation to serious crime. A further UN draft resolution in 2003 "Cybersecurity and the Protection of Critical Information Infrastructures," cosponsored by Argentina, Bulgaria, Canada, Ethiopia, and the United States, was presented at the 58th session of the General Assembly. If adopted, it invites member states and all relevant international organizations to take into account the need to protect critical information structures from possible misuses, including tracing attacks and, where appropriate, the disclosure of tracing information to other nations (Redo, 2004).

At the international level, the role of agencies such as the United Nations Office of Drug Control and Crime Prevention (UNDCP), Interpol, the Organization for Economic Cooperation and Development (OECD), and the G8 group of nations and regional bodies such as the European Union (EU), Organization 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

P1: NPP
JWBS001B-84.tex WL041/Bidgoli WL041-Bidgoli.cls October 17, 2005 12:27 Char Count= 0

cross-border cooperation in policing. As digital technology becomes more pervasive and interconnected, ordinary crime scenes will contain some form of digital evidence. Crucially many cybercrimes take place across jurisdictional boundaries with offenders routing attacks through various jurisdictions that can only be countered by a cross-border and international policing response.

The digital divide between nation states is growing rapidly and the role of advanced information technology-based economies in bridging this divide is essential. Most developing countries do not have a telecommunications sector capable of supporting information and communication technologies (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, whereas 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 gross domestic product (GDP) and 93% of Internet users, whereas the bottom fifth have 1% of GDP and only 0.2% of Internet users (United Nations, 2003, as cited in Redo, 2004—see also volume II, chapter 88).

The need for reliable and efficient mechanisms for international cooperation in law enforcement matters has never been more urgent. 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 cybercrime. This chapter considers some of the avenues for cooperation. However rapid the growth of ICT may be, it is unlikely to continue its apparently exponential trajectory unless the digital divide is broken and poorer nations and neighbors are included.

There is also growing concern about the potential for misuse of information technology (IT) by terrorists. This has made cyberterrorism a major strategic issue in the prevention of terrorism because the technologies themselves may be attacked and can also be used to support terrorism in the same way ITs are used by predatory cybercriminals. The use of computers by terrorists to plan, organize, and communicate is well documented and counterterrorism 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 have been used to gain access to sensitive law enforcement information (see International Narcotics Control Board, 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).

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 publicized 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 combined the effects of a worm, spreading rapidly across the Internet, with that of a distributed denial of service attack in which computing power is directed at a target system with a view toward 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, Shannon, Voelker, & Savage, 2003; Semple, 2004; Staniford, Paxson, & Weaver, 2002; see also volume III, part 1).

The U.S. Federal Bureau of Investigation (FBI) has also stressed that critical infrastructure protection is a priority in the United States. Given that most elements of critical infrastructure such as power generation, telecommunications, transport, and financial institutions are owned by the private sector, cooperation between law enforcement and the private sector is obvious. To help bridge the public–private gap, the FBI has introduced its Infraguard Program with over 4,000 members (Iden, 2003). There is also a crucial role for the communications and IT industries in designing products that are resistant to crime and that facilitate detection and investigation.

What Is Computer Crime?

The scope of criminal activities and their social consequences can be summarized by a typology of computer-related crime that comprises the following: conventional crimes in which computers are instrumental to the offense, 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 list (by no means exhaustive—see Part 2 for further details):

- Interference with lawful use of a computer: cybervandalism and terrorism; denial of service; insertion of viruses, worms, and other malicious code.
- Dissemination of offensive materials: pornography or child pornography, online gaming or betting, racist content, treasonous or sacrilegious content.
- Threatening communications: extortion, cyber-stalking.
- Forgery or counterfeiting: ID theft; internet protocol (IP) offenses; software, CD, DVD piracy; copyright breaches; and so forth.
- Fraud: payment card fraud and e-funds transfer fraud; theft of Internet and telephone services; auction house and catalog fraud; consumer fraud and direct sales (e.g., virtual snake oils); online securities fraud.
- Other: Illegal interception of communications, commercial or corporate espionage, communications in

P1: NPP
JWBS001B-84.tex WL041/Bidgoli WL041-Bidgoli.cls October 17, 2005 12:27 Char Count= 0

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 cybercriminals and bringing them to justice pose challenges to law enforcement agencies across the globe and require a degree and timeliness of cooperation that has been until only recently regarded as impossible to achieve. However, computer intrusion is now more likely a predicate to a more serious offense. Forensic computing and evidence preservation protocols are essential to effective investigation and prosecution, especially given the trans-border nature of evidence collection (Pollitt, 2003; and see volume II, part 3, chapters 124–129). 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 online situations, 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 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 to undertake the crime. Consequently, efforts to reduce online offenses and e-commerce crime need to recognize 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 online. Risk-aversive systems of e-commerce therefore needed to be far more integrated than conventional environments and require more than passing attention to what the information security engineers like to call social engineering (see also volume III, part 2).

TRANSNATIONAL POLICING AND CYBERCRIME

The transnational nature of cybercrime reflects the process of globalization, which has intensified over the past two decades. The emergence of e-commerce, as well as the social dimension of the Internet and associated cybercrimes, 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 globalization 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 globalization, substate actors, such as large commercial institutions, play a crucial role in the emergence of what Sheptycki (2000) terms a transnational-state system. Consequently the role of public–private police partnerships in the marketplace and the emergence of civil society on the Internet combined with public awareness are essential to contain cybercrime among ordinary users.

Although 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 cybercrimes 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 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 cybercriminals. The compatibility of criminal activity with these global changes is illustrated by the expansion and convergence of the profitable business of smuggling of humans, narcotics, or other illicit commodities with the development of communication infrastructure and trade.

The passage of the Council of Europe's Cybercrime Convention in December 2001 and its activation in July 2004 provides an international legal mechanism for cooperation in law enforcement and harmonization of laws (see Cross, 2003; Csonka, 2005; Esposito, 2004, Sato 2004), although 37 states have signed the convention and the "First Additional Protocol to the Convention on Cybercrime on the Criminalisation of Acts of a Racist or Xenophobic Nature Committed through Computer Systems" has been signed by 22 states but is yet to be ratified (see "Additional Protocol to the Convention on Cybercrime," 2003).

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 the real-time collection of traffic data, and to intercept the content of questionable electronic data. A number of countries outside the Council of Europe (United States, Mexico, Japan, Canada, and South Africa) were involved from the outset and have signed the convention, and many other countries, notably in South America, are considering similar model legislation (see OAS, n.d., for recommendations on an inter-American cybercrime instrument). The convention is also open to any nonmember state wishing to join (via a request to the Committee of Ministers of the Council of Europe). Given the pressing need for a broader multilateral structure for cross-border cooperation in the computer crime area,

P1: NPP
JWBS001B-84.tex WL041/Bidgoli WL041-Bidgoli.cls October 17, 2005 12:27 Char Count= 0

every effort should be made to open up the convention for accession by a wide number of signatories as soon as is practicable (Bullwinkel, 2005). Indeed many jurisdictions in the Asian region, Thailand in particular, have looked at the convention for guidance in formulating national laws.

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 cybercrime activity compels police partnerships with banks, telecommunication providers, and corporations. Partnerships also raise real issues of shared intelligence in environments of trust. Thus, the mobilization of so-called private police and non-governmental organizations in partnership with public police are essential if cybercrime is to be contained. Crime exploits the gaps in the sovereign state system of international relations and unless that is recognized in communities of shared fate, coordinated forms of regulatory endeavor (free, for example, from unduly strict or pedantic definitions of dual criminality) may be the only means to curtail cybercrime and its inevitable cross-border dimension.

United Nations Convention against Transnational Organized Crime

Since the early 1990s, beginning with the Eighth 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 cybercrime. The scope of computer-related crime affects every country in the United Nations, and the UN General Assembly in 2001 promoted new international efforts to assist member states in dealing with computer-related crime. The General Assembly, in the "Plans of Action for the Implementation of the Vienna Declaration on Crime and Justice: Meeting the Challenges of the Twenty-first Century" (General Assembly 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 again addressed the Vienna Plan of Action (General Assembly 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 consider the plan. In 2001, the UN secretary-general explored various options for further work on high-technology and computer-related crime and considered the following four questions: 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 Organized 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).

Although not specifically directed at cybercrime, the complementary role of the TOC Convention is a highly relevant global instrument for addressing some of the more nefarious aspects of cybercrime. The TOC Convention was introduced in December 2000 in Palermo, Italy. The TOC Convention has been signed by 147 states (and 82 parties) and came into force on September 23, 2003 (see "United Nations Convention," n.d.). The TOC Convention significantly extends the reach of the 1988 Vienna Convention against Illicit Traffic in Narcotics and Psychotropic Substances. The TOC Convention enables MLA between states and establishes several offense categories: participation in an organized 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 January 28, 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 organized 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; refers to provisions for training and materials, especially assistance for developing countries; and places obligations on capable states. The 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 cybercrime, in line with Article 13.1(a) of the UN Charter emphasizing 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 offenses signatories are obliged to criminalize (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 *organized criminal group* reflect an understanding that organized criminal activity is no longer confined to a relatively narrow range of offenses traditionally associated with organizations such as Triads and the Cosa Nostra. The TOC Convention defines an offense 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 organized 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 cybercrime therefore qualify as serious crime because such offenses usually affect more than a single jurisdiction, often involve at least three or more actors, and are

P1: NPP
JWBS001B-84.tex WL041/Bidgoli WL041-Bidgoli.cls October 17, 2005 12:27 Char Count= 0

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 and 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 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 cybercrime 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 offenses 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 offenses), the TOC Convention will substantially expand the range of extraditable offenses between them (Bullwinkel, 2005; Cross, 2003).

THE COUNCIL OF EUROPE CYBERCRIME CONVENTION

The Council of Europe, founded in 1949, comprises 45 countries, including the members of the European Union (a distinctly 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 organizations 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 cybercrime, which completed its work late in 2001.

The resulting Cybercrime Convention has three aims: to lay down common definitions of certain criminal offenses—nine are mentioned in the convention—thus enabling relevant legislation to be harmonized 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 criticized 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 Cybercrime obligates signatories to criminalise a minimum list of specific offenses for which there was consensus and thus harmonized offenses to eliminate problems of dual criminality. The basic structure and content of the convention is outlined below.

Computer-Related Offenses

Title 1 addresses offenses against the confidentiality, integrity, and availability of computer data such as (1) illegal access of a computer system; (2) interception of nonpublic 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. Criminalizing 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 and 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 offenses, such as computer-related fraud or forgery. The criminalization of illegal interception protects the privacy rights of data communication, 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 and also captures malicious codes and viruses (e.g., Trojan horses).

The convention criminalizes 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 offense 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

P1: NPP
JWBS001B-84.tex WL041/Bidgoli WL041-Bidgoli.cls October 17, 2005 12:27 Char Count= 0

purposes are not included. This offense therefore requires a particular purpose: that is, committing any of the other offenses against the confidentiality, integrity, and availability of computer systems or data.

Title 2 covers the traditional offenses 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). Chapter 5 obliges signatories to criminalize the attempt to commit certain offenses on which the convention imposes a criminalization obligation, as well as aiding and abetting the commission of offenses, and also provides for the liability of legal persons.

Content-Related Offenses

Title 3 seeks to control the use of computer systems as a vehicle for the sexual exploitation of children and acts of a racist or xenophobic nature. This category of offenses concerns the subject or contents of computer communications and focuses on offenses related to children. The convention makes various acts (from the possession to the intentional distribution of child pornography) criminal offenses, thus covering all links in the chain. This provision criminalizes various aspects of the electronic production, possession, and distribution of child pornography. Most states already criminalize 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 exploitation. Other types of illegal content, such as racist propaganda, have also been included but in the form of an additional protocol criminalizing racist propaganda. Esposito (2004) notes that cybercrime is now defined as crimes committed against and through computer systems. The CoE's Cybercrime Convention was originally intended to cover only the first category, although there is a growing consensus, at least in Europe, of the need to address the second category (e.g., Article 9 of the Cybercrime Convention on cyber-pedopornography and the additional protocol on the fight against racism and xenophobia on the Internet).

Offenses Related to Copyright Infringement

Title 4 criminalizes willful 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 offenses on the Internet and cause concern both to copyright holders and to 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 offenses, for example to determine the place where the offense 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 offenses 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.

GLOBAL AND REGIONAL COOPERATION

Cybercrime 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 offenses take place for the purpose of determining criminal jurisdiction. An offense may produce victims in many countries, as in cases involving virus attacks, copyright violations, and other offenses 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, and see volume II, part 2, chapters 92 and 93).

Most countries have domestic statutes relating to legal assistance and extradition and these sometimes enable extensive cross-border cooperation even in the absence of a formal treaty relationship. However, domestic legislation, while helpful for certain types of cooperation, is not a substitute for well-developed bilateral (or multilateral) agreements. For example, in the absence of a treaty establishing a direct relationship between legal authorities, requests for legal assistance must often be transmitted through the cumbersome and time-consuming diplomatic channel and this method is too slow to meet the challenges of cybercrime. Bilateral agreements such as MLA treaties and extradition treaties are more reliable means for international cooperation in criminal matters. Extradition treaties fall into two general categories: so-called list treaties and more modern dual criminality treaties.

P1: NPP
JWBS001B-84.tex WL041/Bidgoli WL041-Bidgoli.cls October 17, 2005 12:27 Char Count= 0

In the case of list treaties, the contracting parties are bound to extradite only those offenses specified in the agreement. This may be a significant limitation, particularly in cases involving newer forms of crime (including many cybercrimes). The trend in modern treaty practice is to provide for extradition for offenses punished by imprisonment for more than a year under the laws of both parties. These dual criminality extradition treaties are as broad as the criminal laws of the requesting state but extradition for cyberoffences may prove difficult, because some jurisdictions have not yet criminalized the conduct. When this occurs the requested state should follow the practice, accepted in international law, of interpreting the treaty in favor of extradition. The advantages of a bilateral treaty are that they limit the requested state's discretion to refuse assistance. In bilateral MLA treaties, the parties will in most cases be required to execute the request unless the request relates to a political offense or to an offense under military law that would not be an offense under ordinary criminal law or when the request would prejudice the requested state's security or similar essential interests. Subject to limited exceptions and the overall scope of the agreement, bilateral treaties ordinarily oblige the signatories to provide a wide measure of assistance and often the requested assistance must be provided even in the absence of dual criminality (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 harmonization and fewer opportunities for transnational criminals to exploit jurisdictional and legal loopholes between nations. 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 cybercrime, low-intensity warfare, and terrorism.

Regional efforts outside of Europe are also underway via OAS, ASEAN and the APEC forum. Such developments have yet to evolve into fully institutionalized 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 organizations, apart from the United Nations and the Council of Europe, involved in developing international and regional efforts against cybercrime are briefly described in the following sections.

G8 Senior Experts Group on Transnational Organized Crime

The Group of Eight (comprising Canada, Germany, France, Italy, Japan, the United Kingdom, the United States and, since 1995, Russia), although originally established to coordinate economic policy, has also 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 organized crime. In 1996, the Lyon Group devised 40 recommendations aimed at increasing the efficiency of collective action against transnational organized 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 40 recommendations cover a range of issues and emphasized 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 2004, 39 countries participated in the global 24/7 cybercrime response network. Later, G8 ministers endorsed a set of principles and an action plan to respond to transnational cybercrime cases that included provision of adequate personnel and training to fight high-tech crime; domestic laws that criminalized cybercrime 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 cybercriminals. The 1999 Moscow meeting later endorsed principles on transborder access to stored computer data and called for a comprehensive response to Internet fraud and more industry coordination. Most recently, 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" (G8 Justice and Home Affairs Communiqué 2004).

ASEAN

ASEAN comprises 10 nations: Brunei Darussalam, Cambodia, Indonesia, Laos, Malaysia, Myanmar, Philippines, Singapore, Thailand, and Vietnam. Although 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, but the 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 in partnership with the UNDCP illustrates

P1: NPP
JWBS001B-84.tex WL041/Bidgoli WL041-Bidgoli.cls October 17, 2005 12:27 Char Count= 0

the quickening of MLA responses to transnational crime such as cybercrime. ASEAN has conducted four ministerial meetings on problems of transnational crime (Manila 1997, Yangon 1999, Singapore 2001, and 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. 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 organized 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 Meetings 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 ("Joint Communique of the Third ASEAN Ministerial Meeting," 2001). As noted, the ASEAN anticrime 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, established under the Treaty of Maastricht in 1992. The European Union has 28 member states and recently completed the accession of 13 countries in eastern and southern Europe (with some new members joining on May 1, 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 Cybercrime Convention and EU conventions on mutual assistance in criminal matters and extradition (see European Union, Judicial Cooperation in Criminal Matters, 1998 and see generally http://europa.eu.int/scadplus/leg/en/s22004.htm visited May 9, 2005), 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 (Decision establishing Eurojust, 2002). Further strengthening of MLA is contained in the April 19, 2002, "Proposal for a Council Framework Decision on Attacks against Information Systems", adopted in June 2003 (European Union, 2003)

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 organized crime. Based in Brussels, Europol is accountable to the EU's Council of Ministers for Justice and Home Affairs. The organization is comprised of European liaison officers (who represent national law enforcement agencies across the European Union, 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 was recently extended to include the fight against cybercrime. 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 European Union. In addition, it is likely Europol will eventually assume a greater investigative and operational role.

The Organization for Economic Cooperation and Development

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 the 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 cybercrime 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 September 11, 2001, OECD governments developed a series of guidelines designed to counter cyber-terrorism, computer viruses, hacking, and related threats ("OECD Governments Launch Drive," 2002). 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 intergovernmental law enforcement coordination that offers a template for transnational cooperation against cybercrime is the Financial Action Task Force (FATF) established at the G7 Paris Summit in 1989 and based in the OECD. FATF is a policy-making body whose aim is the implementation of legislative and regulatory reforms needed to combat money laundering. In 1990, 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

P1: NPP
JWBS001B-84.tex WL041/Bidgoli WL041-Bidgoli.cls October 17, 2005 12:27 Char Count= 0

undertaken by FATF, a number of FATF-style organizations have also developed at the regional level including, in the Asian-Pacific region, the Asia/Pacific Group on Money Laundering, established in 1997, which 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 Organization, 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 organizations 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 recognized the need for law enforcement officials to acquire specialized 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 organized working groups comprising local experts in computer-related crime who meet periodically to share experiences and develop best practices (Noble, 2003). An example is the Asia-South Pacific Working Party on Information Technology Crime that currently meets annually and has undertaken projects relating to the handling of digital evidence, forensic tools, and training. Interpol has also endeavored 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 organized crime). In addition, Interpol has increased its focus on intellectual property-related crime, because sophisticated and well-financed organized criminal groups increasingly carry out these offenses 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 Web site. 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 be better trained and equipped. This cooperation strengthens police capacity to respond to the theft of payment cards and other computer-related crimes that reduce the integrity of the market and limit the social benefits of Internet communications. 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).

APEC

Founded in 1989 in Canberra, Australia, for the purpose of promoting economic growth among member states, APEC now consists of 21 member economies. 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) into a number of areas relevant to cybercrime enforcement, including an Intellectual Property Rights Working Group, an Electronic Commerce Steering Group (ECSG; see generally http://www.apecsec.org.sg/workgroup/e-commerce. html) and the work of the Council for Security Cooperation Asia and Pacific (2004). 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 implicates 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 cybersecurity laws, on a par with existing international standards, particularly the CoE Cybercrime Convention and UN General Assembly Resolution 55/63 of 2000; identify or create national cybercrime units and international high-technology assistance contact points; and establish computer emergency response teams that exchange threat and vulnerability

P1: NPP
JWBS001B-84.tex WL041/Bidgoli WL041-Bidgoli.cls October 17, 2005 12:27 Char Count= 0

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 cybercrime, 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 offenses and cybercrime showed that although some states had enacted new laws, many remained ill-equipped to deal with the cross-border nature of these offenses. Orlowski (2004) also reported an APEC cybercrime legislation survey involving 14 nations that found all had some legislative provisions to address cybercrime 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 offenses 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 offenses 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 cybercrime. 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 Cooperation

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) outlined the basic elements of an effective regime for regional cooperation in combating cybercrime 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 cybercrime
- Broadly criminalize the conduct (including juvenile offenders) and focus on all violators big and small
- Strengthen international initiatives by updating existing treaties and agreements to recognize the existence, threats, and transnational nature of high-tech computer-related crimes and strive for legal harmonization
- The development of forensic computing skills by law enforcement and investigative personnel and mechanisms for operational cooperation between law enforcement agencies from different countries, that is, 24/7 points of contact for investigators.

In the future, organized crime may be expected to recruit IT specialists, intimidate corporate insiders to obtain access to IT systems, and use anonymizers and encryption in furtherance of cybercrime. In addition, there is evidence of the deployment of intelligent malicious software designed to elude detection by antivirus software. 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 and provide data (such as customers' records) for extortion and denial-of-service offenses. Most significant, 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 organized 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 online information from members of the public relating to questionable online activities that 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.

Many nations and regional bodies such as the Council of Europe have addressed the problem of cybercrime and laws exist that criminalize the unauthorized access and unlawful use of computers, but such laws are neither universal nor uniform. Concerns remain focused on the

P1: NPP
JWBS001B-84.tex WL041/Bidgoli WL041-Bidgoli.cls October 17, 2005 12:27 Char Count= 0

weakest links in the supposedly seamless security chain necessary to prevent cybercrime by predatory criminal groups. Comity thus can only be ensured if wealthy states and affected industries are prepared to extend aid to those less capable states or agencies. 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 overregulation could stifle commercial and technological development. Those skeptical of a heavily interventionist approach also argue that the marketplace may at times be able to provide more efficient solutions than the state to the problems of computer-related crime.

Although there is consensus about the risks of computer-related crime, apart from criminalizing 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 in which 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. Cybercrime 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 and 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. Microsoft Corporation has now, it seems, reflected on its failure to lead the market in respect to consumer safety and to recognize that the market demands a secure and trusted environment if computers and information technology are to realize their full potential.

In conclusion, controlling crime involving digital technology and computer networks will 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 five years, considerable progress has been made within and between nations to develop the capacity of police to respond to cybercrime. But the pace of technological change will continue unabated and the adaptability of cybercriminals will continue to pose challenges for law enforcement. The extent of transnational law enforcement cooperation achieved thus far, promising though it may be, can only be regarded as a beginning.

GLOSSARY

Comity An association of civility and mutual benefit among nations, especially in regard to the recognition of the laws and customs of other nations.

Dual Criminality A rule governing or limiting the reach of a bilateral or multilateral treaty or convention, or a cross-border law enforcement that authorizes assistance only if the offense is criminalized in the law of both states.

Extradition The formal arrangements between nations that allow fugitives, suspects, or witnesses in one country to be transported to the country in which the crime was committed.

List Treaty A bilateral or multilateral treaty providing extradition or other legal assistance such as the seizure and preservation of evidence that is limited to the list of offenses.

Mutual Legal Assistance The general term for all informal and official forms of police, legal, and criminal justice cooperation between states usually provided on a reciprocal basis.

Social Engineering The manipulation of human behavior for the purposes of revealing passwords, source code, and other confidential information without recourse to unauthorized access to a computer system by means of exploiting or intrusion software.

CROSS REFERENCES

See *Cyberterroism and information Security; Global Aspects of Cyberlaw; Law Enforcement and Computer Security Threats and Measures; Law Enforcement and Digital Evidence; Privacy Law and the Internet*.

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 R. Broadhurst (Ed.), *Proceedings of the Asia Cyber Crime Summit*. Hong Kong: Centre for Criminology, University of Hong Kong, pp. 133–140.

Bullwinkel, J. (2005). International cooperation in combating cyber-crime in Asia: Existing mechanisms and new approaches. In R. Broadhurst & P. Grabosky (Eds.), *Cyber-crime: The challenge in Asia*, pp. 269–302. Hong Kong: University of Hong Press.

Council of Europe. (2003, January 28). *Additional Protocol to the Convention on cybercrime on the criminalisation of acts of a racist or xenophobic nature committed through computer systems*. Retrieved August 9, 2004, from http://conventions.coe.int/Treaty/en/Treaties/Html/189.htm

Council for Security Cooperation Asia and Pacific. (2004). *Cybercrime and its effects on the Asia Pacific region: Report of the Transnational Crime Working Group*. Retrieved August 4, 2004, from http://www.police.govt.nz/events/2001/e-crime-forum/cybercrime_and_its_effects.html

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*, pp. 25–36. Hong Kong: Hong Kong Police Printing Department HKSAR.

Csonka, P. (2005). The Council of Europe Convention on Cybercrime: A response to the challenge of the New Age? In R. Broadhurst & P. Grabosky (Eds.), *Cybercrime: The challenge in Asia*, pp. 303–326. Hong Kong: University of Hong Press.

Decision establishing Eurojust (2002, 28 February). Retrieved May 9, 2005, from http://europa.eu.int/scadplus/leg/en/lvb/l33188.htm

Esposito, G. (2004). The Council of Europe Convention on Cyber-crime: A Revolutionary Instrument? In R. Broadhurst (Ed.), *Proceedings of the 2nd Asia Cyber Crime Summit*. Hong Kong: Centre for Criminology, University of Hong Kong, pp. 54–64.

European Union, (2003). Framework Decision. Retrieved May 9, 2005, from http://europa.eu.int/information_society/eeurope/2005/all_about/mid_term_review/security/index_en.htm

European Union (1998 June, 29) Judicial Cooperation in Criminal Matters. Retrieved May 9, 2005 from http://europa.eu.int/scadplus/leg/en/lvb/l33055.htm

G8 (2004, May 11), Justice and Home Affairs Communiqué, Washington. Retrieved December 11, 2004 from www.g7.utoronto.ca/justice/justice040511_comm.htm

Grabosky, P., & Broadhurst, R. (2005). The future of cybercrime in Asia. In R. Broadhurst & P. Grabosky *(Eds.), *Cyber-crime: The challenge in Asia,* pp. 347–360. Hong Kong: University of Hong Kong Press.

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*, pp. 69–73. Hong Kong: Hong Kong Police, Printing Department HKSAR.

International Narcotic Control Board. (2001). *Report of the International Narcotic Control Board 2001* (UN E/INCB/2001/1). Vienna, Austria: Author.

Johnston, L. (2000). Transnational private policing: The impact of global commercial security. In J. W. E. Sheptycki (Ed.), *Issues in transnational policing*, pp. 21–42. London: Routledge.

Joint Communique of the Third ASEAN Ministerial Meeting on Transnational Crime. (2001, October 11). Retrieved November 21, 2003, from http://www.aseansec.org/5621.htm

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*, pp. 44–50. Hong Kong: Hong Kong Police, Printing Department HKSAR.

Moore, D., Shannon, C., Voelker, G. M., & Savage, S. (2003). *Internet quarantine: requirements for containing self-propagating code*. Paper presented at the meeting of the IEEE INFOCOM, San Francisco, CA.

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

Newton, J. (2004). Interpol and the cards industry: Global partnerships to deliver local solutions. In R. Broadhurst (Ed.), *Proceedings of the 2nd Asia Cyber Crime Summit*. Hong Kong: Centre for Criminology, University of Hong Kong, pp. 124–127.

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*, pp. 37–43. Hong Kong: Hong Kong Police, Printing Department HKSAR.

OECD *governments launch drive to improve security of online networks*. (2002, August 7). Retrieved from http://www.oecd.org/document/53/0,2340,en_2649_201185_1946997_1_1_1_1,00.html

Organization of American States. (n.d.). *Group of experts and cyber crime*. Retrieved October 11, 2004, from http://www.oas.org/juridico/english/cyber.htm

Orlowski, S. (2004). APEC activities to address cybercrime through public/private cooperation. In R. Broadhurst (Ed.), *Proceedings of the 2nd Asia Cyber Crime Summit*. Hong Kong: Centre for Criminology, University of Hong Kong, pp. 37–45.

Pollitt, M. (2003). Digital evidence in Internet time. In R. Broadhurst (Ed.), *Bridging the GAP: A global alliance on transnational organised crime*, pp. 82–85. Hong Kong: Hong Kong Police, Printing Department HKSAR.

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. 117–139.

Redo, S. (2004). The UN. In R. Broadhurst (Ed.), *Proceedings of the 2nd Asia Cyber Crime Summit*. Hong Kong: Centre for Criminology, University of Hong Kong, pp. 18–29.

Sato, T. (2004). Countermeasures against cyber-crime in Japan. In R. Broadhurst (Ed.), *Proceedings of the 2nd Asia Cyber Crime Summit*. Hong Kong: Centre for Criminology, University of Hong Kong, pp. 139–145.

Semple, K. (2004, January 27). E-mail worm snarls computers around globe. *New York Times*. Retrieved January 28, 2004, from http://www.nytimes.com/2004/01/27/technology/27CND-VIRU.html

Sheptycki, J. W. E. (Ed.). (2000). *Issues in transnational policing*. London: Routledge.

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

Sussmann, M. A. (1999). The critical challenges from international high-tech and computer-related crime at the millennium. *Duke Journal of Comparative and International Law, 9,* 451–473.

United Nations. (2003). *World public sector report 2003: E-government at the Crossroads, Sales No. E.03.II.H.3*. New York: Author.

United Nations convention against transnational organized crime. (n.d.). Retrieved August 9, 2004, from http://

P1: NPP
JWBS001B-84.tex WL041/Bidgoli WL041-Bidgoli.cls October 17, 2005 12:27 Char Count= 0

www.undcp.org/crime_cicp_signatures_convention.html, visited August 9, 2004.

Urbas, G. (2005). Cyber-crime legislation in the Asia-Pacific region. In R. Broadhurst & P. Grabosky (Eds.), *Cyber-crime: The challenge in Asia*, pp. 207–242. Hong Kong: University of Hong Press.

European Union, http://www.europa.eu.int/scadplus/leg/en/lvb/114015b.htm; visited December 11, 2003.

European Union, http://www.europa.eu.int/scadplus/leg/en/lvb/133055.htm; visited December 11, 2003

Interpol, http://www.interpol.int/Public/FinancialCrime/IntellectualProperty/Default/.asp