Eleventh United Nations Congress on Crime Prevention and Criminal Justice

Bangkok, 18-25 April 2005

Distr.: General
14 March 2005

Original: English

Item 3 of the provisional agenda[*]
Effective measures to combat transnational organized crime

Workshop 6: Measures to Combat Computer-related Crime[**]

Background paper[***]

Summary

The worldwide proliferation of new information and communication technologies has given rise to more forms of computer-related crime, which pose threats not only to the confidentiality, integrity, or availability of computer systems, but also to the security of critical infrastructure. Furthermore, technological innovation gives rise to distinct patterns of criminal innovation; hence, different threats from computer-related crime mirror differences across the spectrum of the so-called "digital divide". When combating such crime, a number of forensic problems —arising in part from intangible and transient digital evidence—challenge investigators, prosecutors and judges alike. Moreover, effective investigation and prosecution of computer-related crime often require tracing criminal activity and its effects through a variety of Internet service providers or companies, sometimes across national borders, which may result in difficult questions of jurisdiction and sovereignty.

The complexity of the challenges specific to computer-related crime necessitates international cooperation, which ultimately requires countries to be equipped with the necessary legal, procedural and regulatory tools. In order to develop effective methods for efficient international cooperation to combat computer-related crime, a number of regional and interregional efforts have been undertaken in recent years, leading to several significant accomplishments. In order to bring those efforts to fruition, it is necessary to support a wide range of research

[*] A/CONF.203/1.

[**] The Secretary-General wishes to express his appreciation to the Korean Institute of Criminology and the Government of Canada for assisting in the organization of Workshop 6.

[***] Submission of the present document was delayed by the need for additional research and consultations.

on the various aspects involved in combating computer-related crime to foster an active partnership between government and the private sector.

The present background paper highlights the challenges posed by computer-related crime so that the participants in Workshop 6 may consider the recommendations offered by the regional preparatory meetings for the Eleventh United Nations Congress on Crime Prevention and Criminal Justice and chart a course for an effective global response.

Contents

I. Introduction

1. Information and communication technologies are transforming societies throughout the world. Innovation is creating new markets for goods and services. Such technologies are revolutionizing labour processes, enhancing productivity in traditional industries and reshaping the speed and flow of capital. Yet economic changes are only one side of the equation. Societies are also experiencing profound cultural changes—shaping and being shaped by mass media and adapting to the explosive growth of the Internet. The worldwide multiplication of new information and communication technologies also casts a dark shadow: it has made possible new forms of exploitation, new opportunities for criminal activity and indeed new forms of crime.

2. The four regional preparatory meetings for the Eleventh United Nations Congress on Crime Prevention and Criminal Justice proposed a number of recommendations for consideration by the Eleventh Congress, including: (a) to examine current experience and existing national legal frameworks and arrangements for cooperation between States, as well as between States and Internet providers; (b) to examine the most appropriate ways to promote cooperation, exchange of expertise, knowledge and know-how between Governments and the private sector for the establishment and operation of mechanisms for preventing and controlling computer-related crime and ensuring the security of computer networks and communication systems and the existence of appropriate response mechanisms; (c) to explore ways and means of enhancing the capacity of Governments to develop and apply adequate special investigative techniques and prosecutorial capabilities, including by developing and establishing comprehensive training programmes for criminal justice officials; (d) to deal with the use of computerized technology in exploiting women and children, especially in relation to pornography and paedophilia; (e) to examine the feasibility of establishing a global Internet task force for international cooperation in efforts to fight computer-related crime; and (f) to consider proposing the negotiation of a new convention against cybercrime with a view to creating the basis for effective collective action against this form of criminal activity.[1]

The conceptualization of "computer-related crime" or similar terms such as "cybercrime" has been a topic of debate for the past 30 years. The prototype dates back to a report by the Stanford Research Institute;[1] it reappeared in slightly modified form in 1979[2] and in 1989.[3] The organizing schema was widely used in subsequent articles on cybercrime: the computer as subject of a crime; the computer as object of a crime; or the computer as instrumentality (the fourth role, proposed in 1973, the computer as symbol, seems to have disappeared in the 1980s). A useful reformulation of this conceptual model is to regard computer-related crime as conduct proscribed by legislation and/or jurisprudence that (a) is directed at computing and communications technologies themselves; (b) involves the use of digital technologies in the commission of the offence; or (c) involves the incidental use of computers with respect to the commission of other crimes, and hence the computer as a source of digital evidence.[4] Laws and treaties, including the Council of Europe's Convention on Cybercrime,[5] have defined various types of computer-related crime (such as crime against the confidentiality, integrity, or availability of computer systems; content-related offences; and offences related to intellectual property).

II. Computer-related crime

3. There are a number of forms of computer-related crime that target information and communication technologies themselves, sometimes referred to as the class of crimes against the confidentiality, integrity or availability of computer systems. These include forms of theft of telecommunications services and theft of computer services by using diverse hacking techniques (depending on the technology, these include unauthorized access, code and password cracking, digital cloning, credit card skimming and so forth). Servers and websites can be the targets of denial-of-service attacks. In some cases, such crime is the result of distributed denial-of-service attacks in which dozens or hundreds of compromised computers are used as "zombies" to bombard the target with requests that become so numerous that no request can be fulfilled. In other cases, denial of service arises from "packet storms", created by the rampant reproduction of ultra-fast worms (self-replicating computer programs), which in minutes replicate billions of copies of themselves—the sheer volume choking the fattest optical fibre trunks and bringing massive corporate computer systems to a standstill. Global computer virus epidemics have disrupted business and consumer networks for the past two decades; they are periodically punctuated with particularly virulent and damaging new worm and virus strains. Recent examples reveal the two extremes of specialization: at one extreme are worms tailored for a target population numbering tens of millions of computer systems running the most popular operating systems and applications; at the other there are worms designed to attack only high-end security applications running on only a few thousand platforms.

Two residents of Melbourne, Australia, sent between 6 million and 7 million electronic mail (e-mail) messages to addresses in Australia and the United States of America and posted numerous messages on the message boards of major Internet service providers. The purpose of those communications was to encourage the purchase of shares in a United States corporation whose shares were traded in the United States on the National Association of Securities Dealers Automated Quotations (NASDAQ) exchange. The messages, which were sent over false names and relayed through third-party servers, heralded a price increase of up to 900 per cent in the company's shares. Shortly thereafter, the volume of trading in the shares increased 10-fold and its price doubled before trading was halted and the company denied statements made in the various communications.

The two residents were engaged in a classic "pump and dump" scheme: one of the accomplices, a shareholder in the company, knew that he was communicating false information; when the company's share price increased, he sold his shares in the company for a profit.

The two individuals had violated the laws of both Australia and the United States. In addition to stock market manipulation, the volume of traffic generated by the spam e-mail was sufficient to constitute interference with the lawful operation of a computer. The Australian Securities and Investments Commission (ASIC) took action in response to complaints from the Australian public, and information provided by United States authorities. The perpetrators were traced from the trail of e-mail messages distributed through unsuspecting business networks and from the financial trail used to pay for Internet services.

As was customary for offences of this nature, the United States Securities and Exchange Commission sought disgorgement and a temporary and permanent injunction to prohibit the two accomplices from repeating their activities. They were required to relinquish their ill-gotten gains, and to promise never to engage in such conduct again. United States authorities were confident in the capacity of Australia to handle the criminal prosecutions in Australia. ASIC filed 19 criminal charges against the two accused. Both pleaded guilty to disseminating information that was false or materially misleading and likely to induce the purchase of securities and to interfering with, interrupting or obstructing the lawful use of a computer. Both received two-year prison terms, which were suspended (in the principal offender's case, after having spent three months in custody).

4. In the corporate context, deprivation of access to data ranges from circumstances where data may be recoverable (for example, an attack from a disgruntled employee who performs unauthorized encryption of data files), to the unrecoverable destruction of data (meaning not simple deletion of files but physical removal and/or destruction of the hard drives or other storage media containing the files). Wireless local area networks (LANs), which experienced rapid adoption by corporations in recent years, can be vulnerable to denial-of-service attacks (such as jamming) even when they have been secured to prevent unauthorized access.[6]

5. It is also essential to become aware of how computers are used as instruments or tools to commit crime. There are many variants to crime associated with the modification of data—some involving criminal mischief such as electronic vandalism (website defacement) and others constituting professional forgery and counterfeiting. There are websites devoted to "carding" (forging credit cards), which includes making available high-quality counterfeit currency and passports. Theft of data[7] covers a broad spectrum, ranging from information piracy and industrial espionage to copyright infringement (theft of intellectual property in the form of pirate software, MP3 music files, digital video and so on).[8] Theft of data may not be simply an economic crime; it may also infringe upon privacy and related rights of the individual in emerging crimes associated with identity theft.

6. There are many types of computer-related crime involving economic theft, such as hacking attacks on banks or financial systems, as well as fraud involving transfer of electronic funds. There have also been concerns expressed regarding electronic money-laundering and related issues such as tax evasion.

7. Computers are also used to facilitate a wide range of telemarketing and investment fraud involving deceptive practices. Auction fraud is the most widely reported computer-related fraud based on consumer complaints, accounting for 61 per cent of referred fraud complaints, according to a comprehensive report prepared in the United States for the year 2003.[9] Other forms of consumer fraud fall into the more generic category of “non-delivery of goods or payment” following an Internet transaction. Securities fraud, associated with stock market manipulation of low-value investments, is still relatively rare at the consumer level.

A 15 year-old Canadian gained control over a number of computers and used them in distributed denial of service attacks against Yahoo, Amazon.com and other prominent e-commerce sites in February 2000. By slowing or limiting access to those websites, he cost the proprietors millions of dollars in terms of lost business, market capitalization and the cost of upgrading security systems. After boasting of the attacks in Internet chat rooms, the youth was identified by the Federal Bureau of Investigation of the United States, which referred the case to the Royal Canadian Mounted Police. Few if any countries are prepared to extradite juveniles and, in this case, the extradition of a juvenile was precluded under Canadian law. In September 2001, he was sentenced to eight months in a youth detention centre.

8. “Phishing” (or spoofing spam) is the creation of electronic mail (e-mail) messages with corresponding Web pages designed to appear to be existing consumer sites. Like spam, millions of such fraudulent e-mail messages are distributed; however, rather than straightforward solicitation to buy products or services, the e-mails purport to come from banks, online auctions or other legitimate sites and seek to fool users into responding by submitting personal, financial or password data. That personal information is then used for fraudulent purchases (sometimes after the information has been sold to a third party).

9. Existing offences such as extortion (threats to disclose proprietary information or personal information or damage data or systems) and harassment are also being carried out online. There have also been cases of defamation and libel brought forward and successfully prosecuted.

10. There is a range of content-related crimes that involve computers, particularly the dissemination of illegal and harmful material. Of particular concern to the international community has been child pornography. Although child pornography has existed for many decades (in the form of photographs, magazines, films and videos), there has been a growing tendency since the late 1980s for child pornography to be distributed through a variety of computer networks, using a range of Internet services including websites, Usenet newsgroups, Internet Relay Chat

(IRC), and peer-to-peer networks (P2P).[10] Those networks have been used to facilitate exchanges of information, trading in child pornography images or videos, monetary transactions and information with respect to child sex tourism. A certain proportion of the distribution of child pornography is for commercial purposes (rather than non-monetary exchanges among paedophiles) and has been linked to transnational organized crime. There is also a less clearly defined grey zone, where illegality transcends into a generally permissible sphere, given that the Internet has been used for the past 25 years to distribute pornography, much of it legitimate in many jurisdictions and much of it commercial, often referred to as the "adult entertainment industry".[11] Yet there are other cases that are more clearly defined; certain representations constituting pornography (whether in the form of digital images or videos) are deemed to be legally obscene in many countries and the distribution of such obscene material is a crime. The Internet has also been used for other content crimes such as the distribution of hate propaganda and xenophobic material.[12]

Among the best known cases of the 1990s was an attack against Citibank by a young man in the Russian Federation who obtained unauthorized access to the bank's servers in the United States. He enlisted a number of accomplices to open bank accounts around the world, then instructed the Citibank computer to transfer funds to the various accounts. When the scheme was discovered and the alleged perpetrator identified, an arrest warrant was issued by a United States federal court. There was no extradition treaty at the time between the Russian Federation and the United States, but the accused made the mistake of visiting the United Kingdom to attend a computer exhibition. Under the extradition arrangements in force between the United Kingdom and the United States, British authorities could assist as long as the offence with which the accused was charged had some equivalent in British law. The accused applied for a writ of habeas corpus, challenging the extradition by arguing, inter alia, that the appropriation had taken place in the Russian Federation, where his computer keyboard was located, not in the United States. The court held that the physical presence of the accused in St. Petersburg was of less significance than the fact that he was operating on magnetic disks located in the United States. Moreover, the acts with which the accused had been charged had clear equivalents in the Computer Misuse Act 1990 of the United Kingdom; had he been operating from the United Kingdom rather than from the Russian Federation, British courts would have had jurisdiction. The accused was extradited to the United States, where he was convicted and sent to prison.

11. In recent years, there has been increasing attention devoted to the relation between terrorism and the Internet, although here, too, there is a diverse range of activities. There are indications that the Internet is being used to facilitate terrorist financing and as a logistics tool for planning and executing terrorist acts. There is also an increased focus on the role of the Internet in disseminating terrorist propaganda and in the use of the Internet for recruitment. Those activities are

distinct from cyberterrorism, which is defined by the United States National Infrastructure Protection Center as "a criminal act perpetrated through computers resulting in violence, death and/or destruction, and creating terror for the purpose of coercing a government to change its policies".[13] There are two distinct areas of concern: attacks on critical data and attacks on critical infrastructure.

12. There is a growing awareness of the importance of critical information infrastructure, networks that not only make communication possible but also are used to manage and control crucial aspects of other critical infrastructure such as energy, transportation, food and public health. In many countries throughout the world, critical infrastructure may be privately owned and especially vulnerable because many of its distributed control systems and supervisory control and data acquisition systems are connected to the Internet, from where they may be disrupted. Given the growing interdependencies in modern societies, cyber-attacks on such infrastructure can immediately have serious repercussions throughout national economic and political systems, as well as profound transnational effects. It is essential to be able to respond to attacks against critical information infrastructure (whether motivated by terrorism or other criminal activities), in order to minimize the serious risk of potential cascade effects on other critical infrastructure essential to society.

13. The challenges of widely available, strong encryption, which has drawn international attention in the past five years, have not been resolved and the new generation of quantum cryptography is now on the horizon.[14] Although cryptography is essential for business and e-commerce, it has also been utilized by criminals. The "dual-use technology" dilemma extends beyond steganography to varieties of freely available peer-to-peer networking software enhanced with strong encryption that is highly censorship-resistant (such as Freenet). Such technology promotes freedom of expression and could contribute to the furtherance of democratic liberties, but could also be employed by criminals to hide their communications or to distribute illegal material.

III. The digital divide and computer-related crime

14. When information and communication technologies spread to different parts of the world, the dispersion of technology is not uniform. Where one area may be seeing the deployment of high-capacity fibre cables, another could be experiencing the rapid growth of mobile and wireless networks. Dissimilar patterns of technological adaption expose regions to different sets of vulnerabilities, and specific kinds of computer-related crime emerge to take advantage of the different circumstances.

15. The change has been momentous: a staggering sheer increase in the volume of information and communication technology devices (there are now about 2 billion computers and other microprocessor-governed equipment in operation worldwide); the exponential growth in connectivity; revolutionary computing advances such as breakthroughs in miniaturization, speed and storage; the advent of intelligent systems and robotics; and enhanced human-computer interaction. Yet this technological transformation not only pervades the environment, linking people, objects and information in an unprecedented manner, it also brings with it the next

generation of digital threats and vulnerabilities and necessitates a dramatic rethinking of how crime is viewed in the twenty-first century.

16. Aware of this, the General Assembly in 2002 promoted new international efforts to assist Member States in dealing with computer-related crime. In the plans of action for the implementation of the Vienna Declaration on Crime and Justice: Meeting the Challenges of the Twenty-first Century, annexed to Assembly resolution 56/261 of 31 January 2002, one special section is entitled "Action against high-technology and computer-related crime"; in that section, action-oriented policy recommendations are provided for the prevention and control of such forms of crime. In its resolution 57/170 of 18 December 2002, the Assembly invited the Commission on Crime Prevention and Criminal Justice, in formulating recommendations regarding the Eleventh Congress pursuant to Assembly resolution 56/119 of 19 December 2001, to take into account the progress made in the follow-up to the Vienna Declaration and the plans of action.

17. Recognition of the digital divide has been one of the pillars of United Nations' contributions at the outset of the twenty-first century. The overall context is provided by the United Nations Millennium Declaration, adopted by the General Assembly by its resolution 55/2 of 8 September 2000. Under goal 8 of the Millennium Development Goals, annexed to the report of the Secretary-General entitled "Road map towards the implementation of the United Nations Millennium Declaration" (A/56/326), was target 18: "In cooperation with the private sector, make available the benefits of new technologies, especially information and communication". In the Declaration of Principles adopted by the World Summit on the Information Society, held in Geneva from 10 to 12 December 2003, there is a common vision of the information society (A/C.3/59/3, chap. I, sect. A): "We are also fully aware that the benefits of the information technology revolution are today unevenly distributed between the developed and developing countries and within societies. We are fully committed to turning this digital divide into a digital opportunity for all, particularly for those who risk being left behind and being further marginalized."[15]

> By the end of 2004, access to the Internet in China had reached 94 million, or approximately 7.2 per cent of that nation's population, of whom 45.5 per cent were broadband users. It was estimated that there were 41.6 million hosts, 60 million IPv4 addresses, 432,077 domain names and 668,900 cn websites.[16] At an annual growth rate of about 18 per cent, Internet users in China will exceed the number in North America by 2008 and already exceed the number of Internet users in Japan and the Republic of Korea combined. In 1999, there were only 8.9 million users; that number increased to 33.7 million in 2001. The number of hosts grew from 3.5 million in 1999 to 33.7 million in 2001.

18. By the end of 1985, the number of Internet hosts exceeded 2,000; in 1989 it had reached 100,000, and in 1990 it passed the 300,000 mark. It reached 1 million in mid-1992, 10 million in late 1995 or early 1996 and 100 million in late 2000; in

July 2002, the number stood at over 162 million.[17] In 2002, the developing world accounted for only 4.1 Internet users and 3.3 personal computers per 100 inhabitants while the developed world accounted for 33.3 Internet users and 36.2 personal computers per 100 inhabitants (E/2004/62 and Corr.1). The one fifth of the world's people living in the highest income countries accounted for 81.9 per cent of the world's personal computers, 76.2 per cent of the world's Internet users and 97.5 per cent of the world's Internet hosts.[18]

19. Most developing countries do not have a telecommunications sector capable of supporting such dynamic, modern and efficient information and communication systems. In 2000, the United Nations reported that only about 4.5 per cent of the global population had network access, compared with 44 per cent of North Americans and 10 per cent of Europeans, while rates for Africa, Asia, and South America ranged from 0.3 to 1.6 per cent.[19] Currently, more than 98 per cent of global Internet protocol bandwidth, at the regional level, connects to and from North America. Fifty-five countries account for 99 per cent of worldwide spending on information technology production (E/200/52, paras. 50-51). There is a clear trend towards knowledge-based economies, but factors other than development, such as the structure and access costs for telecommunications services, affect rates of access and use.

20. Yet, as the benefits of information and communication technologies begin to be spread more widely, it will also be necessary to increase awareness of the concomitant threats and vulnerabilities associated with computer-related crime. The digital divide not only marks economic differences between developed countries, developing countries and those countries with economies in transition,[20] but also reveals distinct patterns in the threats and vulnerabilities arising from cybercrime. Information and communication technologies are adopted at different times in different regions not simply because of divergences between the rich and the poor, but also because of factors such as regional geography. For example, in some countries with mountainous terrain, the cost of laying underground telecommunications cables may be prohibitive, and setting up microwave relay towers and antenna systems leads to the efficient adoption of wireless telephony networks. As such, the pattern of information and communication technologies in one country or region may be quite distinct from that of a neighbouring country or region. The divergent adoption of technological innovation gives rise to distinct patterns of criminal innovation and hence different threats from computer-related crime.

21. With a minimal telecommunications infrastructure, it is possible for a developing country to be used as a staging ground for attacks or as a transit country through which attacks are routed, particularly if there are no legal sanctions to discourage computer crimes or make such action prosecutable. In the case of developing countries, the kinds of technologies initially deployed and maintained may give rise to threats new to the specific region. Some would suggest that emerging and still fragile information technology structures may be disproportionately vulnerable until the systems become more robust and security standards more ingrained.[21]

22. The type and scale of computers and corresponding networks in corporate or government environments can be quite different from consumer or residential environments. As the adoption of information and communication technologies

begins to increase within the general population, new target groups emerge and become vulnerable to specific sets of computer-related crime, ranging from virus infections and computer intrusions to various forms of consumer fraud. As countries begin to adopt information and communication technologies, different sectors of the society are exposed to different kinds of computer-related crime.

IV. Crossing borders: transborder crime and computer forensics

23. A number of forensic problems must be confronted when investigating computer-related crime. Part of the problem in reconstructing an incident involving a cybercrime is that much of the evidence is intangible and transient. Rather than physical evidence, cybercrime investigations seek out digital traces that are often volatile and short-lived. One of the reasons for the volatility is that some kinds of electronic addressing and routing information (that is, “traffic data”) are not permanently stored. Such information may only remain in the memory of a computer system for a short time and is then overwritten by other routing of information.

24. New technologies create not only novel problems, but also new opportunities for investigators, allowing digital trails to be reconstructed. There are many circumstances in which traffic data and other forms of network management information may be stored in logs rather than simply being overwritten. On the Internet and other computer networks, a variety of network management information is typically stored for subsequent analysis to assist in network accounting, service reliability, network equipment reliability, fault history, performance trends and capacity forecasts. In addition to those purposes, there can also be marketing and consumer profiling uses for such data (for example, requests for pages on retail websites to help determine the most popular products, shopping patterns or customer profiles).

25. There are, however, a number of considerations that determine whether traffic data or similar information will be stored. One factor, for instance, is the type of service. A network access service (for example, using the Remote Authentication Dual-In User Service (RADIUS) protocol) may store certain kinds of subscriber information and some traffic data to permit subscribers to access the Internet. That would be particularly prevalent in time-metered services, which must record when and for how long a subscriber is online. By contrast, it would be minimized in anonymizing or privacy-enhancing services.[22]

26. E-mail, which goes back to the earliest days of the Internet (it was available on ARPANET in 1971), typically contains addressing information and other traffic data in the application header.[23] Some of that information is created by the end-user’s client program and some is created by the e-mail server (running the Simple Mail Transfer Protocol (SMTP)).

27. The most familiar Internet service is probably the World Wide Web, much of which uses the domain name system (DNS) to establish the relationship between domain names (the name of the location of websites) and the Internet Protocol (IP) addresses (the numerical address to and from which packets travel). Web servers may store large amounts of traffic data regarding which pages were requested and

by whom (that is, by which IP address). That practice is more common with commercial servers, as the logging data can quickly reach gigabyte levels and thus be costly to store.

28. File transfer services may or may not collect subscriber information in logs, depending on the implementation. Historically, file transfers were carried out using the file transfer protocol (FTP), although secure transfers are increasingly encrypted using Secure Shell (SSH). Recently, rather than central file servers, the P2P paradigm has emerged; P2P permits file sharing among large numbers of users (decentralized resources distributed across networks of transient entities; examples include Napster, KaZaA, Morpheus, Gnutella and Freenet). Some forms of P2P have easily accessible traffic data, whereas other forms are designed to thwart traffic analysis.

29. Other services include the roughly 100,000 Usenet newsgroups dealing with virtually every topic imaginable. These are accessible through a worldwide network of store-and-forward servers running Network News Transfer Protocol (NNTP)—some traffic data may be available from the server and other data would be on the local personal computer. There are also many forms of real-time chat, ranging from IRC to Instant Messaging.

30. Different Internet services are generally handled by different network devices (such as routers or servers). Depending on how the service provider's site is configured, different logs could be stored on many different machines, potentially controlled by different legal entities and, in some cases, located in different jurisdictions.

31. Given the range of potential services, different market niches and a host of factors including the cost of data retention,[24] it can be said that there is no single business or industry position on the collection and retention of traffic data and subscriber data. It is evident that the retention of certain traffic and subscriber data can facilitate the tracing of criminals over the Internet by law enforcement agencies; some countries have recently adopted legislation compelling mandatory data retention. Even in the absence of laws requiring the retention of traffic data, it is crucial for forensic investigators to understand the range of network accounting and network management practices of Internet service providers to determine the degree to which the requirements of law enforcement agencies may be met by routine Internet service provider practices.[25] The cooperation of Internet service providers may be invaluable when authorities seek to investigate and prosecute computer crime.

32. Effective investigation and prosecution of computer-related crime often requires tracing criminal activity through a variety of Internet service providers or companies with computers connected to the Internet. To succeed, investigators must trace a trail of communications to the source and victim computers or other devices, working with intermediate service providers in different countries. To locate the source of the crime, law enforcement often must rely on historical records that show when, from where and by whom different connections were made. At other times, law enforcement may also need to trace the connection as it is under way. When the providers fall outside the investigator's territorial jurisdiction, which may often be the case, law enforcement would need help from counterparts in other jurisdictions. Traditional and even expedited mutual legal assistance measures are generally

designed to obtain historical and real-time data in cases involving only two countries (for example, the victim's country and offender's country). When a criminal routes communications through three, four or five countries, the legal assistance process takes up successive periods before law enforcement can obtain data from each service provider farther up the trail of communications, increasing the chances that the data will be unavailable or lost, and the criminal will remain unidentified and free to commit future criminal acts.[26]

33. In order to assist the investigation of computer-related crime, the Group of Eight Subgroup on High-tech Crime began preparing in 1997 24-Hour Contacts for International High-tech and Computer-related Crime, a list of computer crime units available to law enforcement agencies 24 hours a day, seven days a week (on a "24/7" basis). The contact network, which currently involves 40 countries, is also an integral part of the Council of Europe Convention on Cybercrime, which offers a set of investigative tools to fight any crime committed against, on and/or through the use of a computer system.

34. With the prevalence of viruses, worms and hackers taking advantage of system vulnerabilities, it is also necessary to have mechanisms in place to make possible immediate responses. Computer Emergency Response Teams (CERTs) have been established in dozens of countries worldwide. Their primary functions are:

(a) To provide a comprehensive view of attack methods, vulnerabilities and the impact of attacks on information systems and networks; provide information on incident and vulnerability trends and characteristics;

(b) To build an infrastructure of increasingly competent security professionals who respond quickly to attacks on Internet-connected systems and are able to protect their systems against security compromises;

(c) To provide methods to evaluate, improve and maintain the security and survivability of networked systems;

(d) To work with vendors to improve the security of as-shipped products.[27]

35. If the perpetrator could be in one country, the attack launched from computers in another country and the effects felt in a third country, it is evident that, in addition to the volatility of data, there are legal challenges arising from problems of borders and jurisdictions. The investigation and prosecution of computer-related crime underscores the importance of mutual legal assistance. Yet questions of sovereignty are only one of the issues that arise in situations of transborder search and seizure. Without appropriate mutual legal assistance there is a risk of unauthorized transborder searches of computer systems by law enforcement officials in one State seeking information in computers located in another State. Before even considering mutual legal assistance, however, it is necessary to reflect on domestic legislation. After all, international cooperation ultimately requires that countries already have in place laws capable of addressing computer crime.

V. National legislation: the necessary prerequisite

36. In some cases, certain types of computer-related crime spread like epidemics oblivious to national borders. In other cases, the elements of crime skip across borders in a careful, premeditated strategy of obfuscation or misdirection. Increasing the density of information and communication technologies in order to reap the benefits of the information society also increases the frequency of domestic computer-related crime. Thus, it is in the interest of economic and public safety that countries introduce domestic legislation to combat computer-related crime.

37. National laws have developed over centuries, while the Internet has developed over mere decades. Of course, the law continues to adapt as society changes. In response to the challenges of computer-related crime, domestic legislation may need to be modernized. Sieber put forward an account of six main waves of computer crime legislation that countries have adopted since the 1970s:[28] (a) data protection and the protection of privacy; (b) criminal law to address computer-related economic crime; (c) protection of intellectual property; (d) protection against illegal and harmful content; (e) criminal procedural law; and (f) legal regulations on security measures such as cryptography and digital signatures.[29]

38. There are a number of elements necessary to address computer-related crime: (a) ensuring that the crimes have been defined in the law; (b) establishing legal investigative powers to combat cybercrime; and (c) pursuing these in a manner that provides safeguards that protect fundamental human rights and freedoms.

A. Substantive offences

39. Comprehensive lists of crime against the confidentiality, integrity and availability of computer systems have been developed.[30] There are also a number of content-related offences (such as the production and distribution of child pornography or xenophobic material) that are included in the class of computer-related crime.

The Information Security Supervision Bureau of the Ministry of Public Security of China reported that just under 5,000 computer crimes were recorded in 2001, up from about 2,900 in 2000 and around 400 in 1999. By mid-2002, the Bureau had reported just over 3,000 cases, and it was estimated that 350 cases of system intrusion and over 800 cases of damage to computer systems would be dealt with by the end of 2002.[31] The number of cases identified by the Bureau was growing at an overwhelming rate, though many cases went unreported or unnoticed. Most offenders were younger people (aged 18-30), and most of the attacks were mounted from Net or cyber-cafes, with offenders hiding their identities by connecting through an http or Sock proxy, by fake IP addresses or by employing cryptography or steganography. Consequently, stronger measures have been taken in the registration and monitoring of cyber-cafes in China.

40. A host of questions have arisen when countries have attempted to adapt provisions designed for physical goods and attempted to use them for the intangible and ephemeral world of digital goods.

41. When drafting provisions, caution should be exercised in order to avoid criminalizing action that would be legitimate. When modernizing a criminal law, there is a fine line between the specific and the general. It is possible that specifically worded provisions can become obsolete when newer technologies become available. Consequently, it is advisable to use “technology-neutral” language.

B. Procedural powers

42. In recent years, because of the increased prevalence of electronic records, many countries have been required to address questions regarding the definition of “documents”. Even basic terms such as the concept of a “place” to be searched can become legal challenges when data are distributed via a computer network (that is, the search may be of a computer in an office in one place but the data may be stored on a computer in another physical place—although “virtually” present to the user and the investigator).

43. When crafting procedural powers, it is helpful to distinguish between three different kinds of information: (a) the actual content of electronic communications; (b) traffic data; and (c) subscriber information. Distinguishing between these three may be advisable because they may attract different expectations of privacy or data protection or trigger other fundamental human rights and freedoms.

44. One of the first legal challenges is to craft a definition of “traffic data” and “subscriber information”. The Council of Europe Convention on Cybercrime,[32] for example, defines traffic data as “any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication’s origin, destination, route, time, date, size, duration, or type of underlying service” (art. 1). The Convention defines subscriber information as “any information, contained in the form of computer data or any other form, that is held by a service provider, relating to subscribers of its services, other than traffic or content data, by which can be established:

“a. the type of the communication service used, the technical provisions taken thereto and the period of service;

“b. the subscriber’s identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement;

“c. any other information on the site of the installation of communication equipment available on the basis of the service agreement or arrangement” (art. 18, para. 3).

45. The issue of definitions was considered in the United Nations Manual on the Prevention and Control of Computer-Related Crime[33] and has also been addressed

in the Council of the European Union framework decision on attacks against information systems, as well as in national legislation.[34]

46. In the domestic legislation of many countries, certain kinds of content may attract higher constitutional protection in the light of concepts such as “private communication” and “freedom of expression”. Thus, it may be necessary to legally and procedurally distinguish the content of certain kinds of Internet communication (those which are not public but private) from traffic data. It is also possible that certain elements of traffic data and subscriber information[35] may, in certain contexts, be linked to data protection provisions because they constitute core biographical information that may attract privacy protection.

47. It should be noted that data collection and subsequent retention are charged with the conflicting interests and values of various stakeholders, and it may be advisable to seek a balance among the diverse legitimate interests. In some jurisdictions collection is tightly constrained under fair information practices, sometimes enshrined in data protection or privacy legislation, pursuant to which data can only be collected for a limited purpose, used only for a stated purpose, with informed consent, and subject to other safeguards on use (such as checks on the integrity of the information, known destruction schedules and subject access).[36]

48. Store-and-forward technologies generally may give rise to distinctive legal questions in those jurisdictions which have different legal regimes for dealing with the monitoring of content in real time (such as wiretapping provisions) as opposed to search and seizure. With respect to computer-related crime, this may be an issue for e-mail, which may require an authorization for monitoring content in real time when the e-mail message is in motion but may require a search and seizure order when it is at rest (that is, stored on the e-mail server or on the end-user’s hard drive). To the extent that the e-mail message is essentially the same in both circumstances, concerns may arise given the recourse to two different legal tools, with potentially two different legal thresholds.

49. There are a number of legal tools that have been developed to assist in computer-related investigations, including preservation orders and production orders. A preservation order is an expedited mechanism that requires service providers to store and save existing data that are specific to a transaction or to a client. Such a procedural mechanism is important in the context of electronic evidence, since such evidence can be deleted or destroyed more easily than physical documents. Essentially, a preservation order is a “do not delete” order. A preservation order[37] is temporary by nature and is made in contemplation of law enforcement agencies securing the necessary lawful authority to obtain the data (such as a warrant to seize the data or a production order to have the data released).

50. A production order requires the custodian of documents to deliver or make available the documents to law enforcement within a specified time period. Production orders are similar to search warrants, although, with a production order, the custodian of the documents conducts the search rather than the police. This type of order is less disruptive, as the custodian is often in a better position to know the exact whereabouts of the documents in question. In the current business environment, it is common for corporations to store data outside the jurisdiction in which they are operating, often to take advantage of cheaper data warehousing costs. A traditional search warrant may be inappropriate in such circumstances,

whereas production orders enable the owner of the data or its custodian to retrieve the documents or records.

VI. Towards solutions through international cooperation

51. It may be necessary to adapt national laws to address cybercrime in order to respond effectively to requests from other States for assistance or to obtain assistance from other States. Compatibility with the laws of other States is an important goal when developing legislation to address computer-related crime. In order to respect the sovereign rights of States and to facilitate international cooperation, it is ultimately necessary to explore the possibilities offered by formal, international mechanisms such as conventions. For mutual legal assistance to function effectively, substantive offences and procedural powers in one jurisdiction should be compatible with those in another.

52. The international community is only now beginning to face the multiple challenges that continue to arise in this field. A massive denial-of-service attack that uses hundreds of compromised computers in several countries to attack commercial websites in another country or the sizeable damage caused by a virus or worm that sweeps across two thirds of the world raises fundamental questions concerning, for example, where the crime was committed and who is to prosecute. Another crucial issue is whether effective action would ultimately depend on which State might have the willingness and capacity to commit itself to investigating and prosecuting. It is evident that transnational computer-related crime is ready to exploit gaps created by divergences in legal frameworks and the capacity of criminal justice systems. Some may regard this as the erosion of sovereignty, whereas others would maintain that the world is witnessing the transformation of sovereignty as information societies begin to emerge around the world.

53. Such scenarios quickly draw attention to the complex issue of extradition, which itself can give rise to a number of problems. For instance, in the absence of functional compatibility of substantive offences, the definition of the crime may be such that dual criminality requirements cannot be met. At the same time, there is a growing acceptance that where dual criminality is required, it is the underlying conduct or the basic elements of the offence that must correspond and not merely the form in which the offence was drafted in the relevant countries. Even if dual criminality does not pose a problem in a specific case, the type of computer-related crime may not be regarded as sufficiently serious (for example, in terms of the associated sentencing provisions) to qualify for extradition.

54. Despite the challenges, however, there have been a number of significant accomplishments since 2000, when the Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders was held, including two new legal instruments: the Council of Europe Convention on Cybercrime; and the United Nations Convention against Transnational Organized Crime, which is global in scope but indirectly deals with cybercrime when carried out by organized criminal groups.

55. At the international level, the role of entities such as the United Nations Office on Drugs and Crime (UNODC), the International Criminal Police Organization (Interpol), the Organization for Economic Cooperation and Development (OECD)

and the Group of Eight and regional bodies such as the European Union, the Council of Europe, the Organization of American States, the Association of South-East Asian Nations and the Asia-Pacific Economic Cooperation (APEC) provide the political and technical expertise necessary to foster international cooperation. Unlike a few years ago, it is now possible to talk about an international consensus on combating cybercrime, especially the transnational forms that it often takes on. Thus, there is finally a positive "moral climate" for concerted action, whether by civil, criminal or administrative measures, and this cooperation recognizes what sociologists call "communities of shared fate".[38]

56. The Convention on Cybercrime was opened for signature on 23 November 2001 and has been signed by 30 States and ratified by 8 States. (The Convention may be signed by States outside of Europe and four non-European States (Canada, Japan, South Africa and the United States) have already signed it.) The Convention came into force on 1 July 2004. It requires States parties to harmonize national laws that define substantive offences. These include offences against the confidentiality, integrity and availability of computer data and systems, as well as computer-related offences such as forgery and computer fraud, offences related to the infringement of copyright, and child pornography offences committed through a computer system. In addition, the Convention foresees an important set of procedural powers, including production orders and preservation orders, designed to facilitate investigation and prosecution in the context of global computer networks. There are also provisions to establish a rapid and effective system of international cooperation. Finally, the issue of "hate crimes" on the Internet gave rise to an additional protocol to the Convention on Cybercrime, to criminalize acts of a racist or xenophobic nature committed through computer systems,[39] which was opened for signature on 28 January 2003. The additional protocol has been signed by 20 States and ratified by two.

57. In 2002, the Commonwealth Law Ministers adopted a model law entitled the Computer and Computer Related Crimes Act.[40] The model law, which shares a common framework with the Convention on Cybercrime, provides law enforcement with effective and modern tools to fight cybercrime. Prosecutors, investigators and legislators can evaluate internationally developed materials such as guidelines, legal and technical manuals, best practices and model legislation to assist authorities in developing domestic legislation.

58. Beginning with the Eighth United Nations Congress on the Prevention of Crime and the Treatment of Offenders, in 1990, the United Nations has been actively involved in addressing various aspects of computer-related developments.[41] In 1994, the United Nations Manual on the Prevention and Control of Computer-related Crime[42] was published with considerable substantive and financial assistance of the Government of Canada and a number of experts from other Governments and non-governmental organizations.

59. In 2000, during the Tenth Congress, a workshop on crimes related to computer networks was held.[43] In 2001, the Secretary-General submitted to the Commission on Crime Prevention and Criminal Justice conclusions of a study on effective measures to prevent and control high-technology and computer-related crime (E/CN.15/2001/4).

60. In 2004, as a result of the first phase of the World Summit on the Information Society, held in Geneva in December 2003, the Secretary-General established the Working Group on Internet Governance to look at spam, cyber-security and other Internet-related issues in preparation for the second phase of the World Summit, to be held in Tunis in November 2005.

61. Computer-related crime is an international phenomenon that requires an international solution. To achieve that solution, the international community should review carefully the means already at its disposal to strengthen international cooperation. It should also seek to augment its knowledge and understanding of the various manifestations of the phenomenon, the challenges those manifestations pose and the feasible and desirable ways to prevent and control the phenomenon.

VII. Cooperation in researching computer-related crime

62. The task of providing an evidence base for future policy development is a challenging one. Research on computer-related crime is in its infancy. Knowledgeable individuals and institutions, in the public and private sectors, may, for commercial, political or national security reasons, be disinclined to share their wisdom with researchers. Information that finds its way to the public record may often be incomplete or inaccurate. Despite those handicaps, it is important to develop a knowledge base, so that efforts to narrow the digital divide can begin to have an effect.

63. A wide range of research methods and comparative approaches need to be employed to provide basic data on the prevalence and severity of the various types of cybercrime. In addition, research on the effectiveness of new laws, policing strategies and prosecution through case review and attrition studies is crucial. Research must not be limited to police or court data and those sources often need to be more specific and uniform. The areas that most urgently require research include victim and offender behaviour, as well as keeping track of legislative and enforcement developments across the globe.[44]

VIII. Public and private-sector cooperation in addressing computer-related crime

64. Increasingly, Governments and representatives of the private sector have recognized the critical need for close collaboration in their efforts to address computer-related crime. No single Government or group of Governments and no single company or industrial sector can succeed on its own; instead, there must be a close partnership of the public and private sector, defined by openness and strong two-way communication. Private-sector entities have played and will continue to play a vital role in the development of technologies to assist in preventing and investigating cybercrime. But, apart from finding technology solutions, the private sector can also play an important role in helping policy makers to identify legislative priorities and solutions. Experience has shown that an active partnership between government and industry can facilitate more effective law enforcement against cybercriminals.

65. It is encouraging that partnerships involving the public and private sectors are multiplying. Members of the Group of Eight have long recognized that an effective response to cybercrime requires unprecedented cooperation between government and industry and have taken important steps in that direction, including by hosting conferences for representatives of government and industry to discuss common concerns and possible solutions.[45] The United Nations, APEC, OECD and other multilateral organizations have likewise made increasing efforts to engage the private sector in such activities.

66. In December 2004, representatives from a number of industries and international law enforcement agencies announced the establishment of Digital PhishNet, a collaborative enforcement operation that unites industrial leaders in technology, banking, financial services and online auctioneering with law enforcement to tackle “phishing”, a destructive and growing form of online identity theft. Digital PhishNet establishes a single, unified line of communication between industry and law enforcement, so that critical data to fight phishing can be compiled and provided to law enforcement in real time. While other industrial groups have focused on identifying phishing websites and sharing best practices and case information, Digital PhishNet is the first group of its kind to focus on aiding criminal law enforcement and assisting in apprehending and prosecuting those responsible for committing crimes against consumers through phishing. Digital PhishNet brings together leaders of industry from 9 of the top 10 United States banks and financial service providers, four of the top five Internet service providers and five digital commerce and technology companies, and works with top federal and international law enforcement agencies.

67. Over the last few years, a number of private-sector entities have teamed with the University of Hong Kong to hold a number of major cybercrime conferences. Those events have brought together senior justice and law enforcement officials from Asia and the Pacific, as well as prominent academics and representatives of leading multilateral organizations, including the United Nations, the Council of Europe, Interpol and APEC. Areas of discussion have included network security challenges, threats to electronic commerce (e-commerce) such as spam, phishing and other forms of online fraud, and online piracy.

68. Law enforcement officials from around the world have over the last several years worked alongside a number of well-known companies to investigate and prosecute online fraudsters and other cybercriminals, including some of the world’s best known spammers.

69. Despite this progress, more could be done to further increase the level of collaboration between government and industry and to provide greater structure and regularity to dialogue and partnerships involving the public and private sectors.

IX. Recommendations

70. The Eleventh Congress may wish to consider the following recommendations, formulated in two meetings of experts hosted by the Korean Institute of Criminology in Seoul, taking also into account the relevant recommendations of the regional preparatory meetings for the Eleventh Congress:

(a) A broad, inclusive focus is necessary to address problems of cybercrime, going beyond criminal law, penal procedures and law enforcement. The focus should include requirements for the secure functioning of a cyber-economy optimizing business confidence and individual privacy, as well as strategies to promote and protect the innovation and wealth-creating potential and opportunities of information and computing technologies, including early warning and response mechanisms in case of cyberattacks. Behind the prevention and prosecution of computer-related crime looms the larger challenge of creating a global culture of cybersecurity, addressing the needs of all societies, including developing countries, with their emerging and still vulnerable information technology structures;

(b) International cooperation at all levels should be developed further. Because of its universal character, the United Nations system, with improved internal coordination mechanisms called for by the General Assembly, should have the leading role in intergovernmental activities to ensure the functioning and protection of cyberspace so that it is not abused or exploited by criminals or terrorists. In particular, the United Nations system should be instrumental in advancing global approaches to combating cybercrime and to procedures for international cooperation, with a view to averting and mitigating the negative impact of cybercrime on critical infrastructure, sustainable development, protection of privacy, e-commerce, banking and trade;

(c) All States should be encouraged to update their criminal laws as soon as possible, in order to address the particular nature of cybercrime. With respect to traditional forms of crime committed through the use of new technologies, this updating may be done by clarifying or abolishing provisions that are no longer completely adequate, such as statutes unable to address destruction or theft of intangibles, or by creating new provisions for new crimes, such as unauthorized access to computers or computer networks. Such updating should also include procedural laws (for tracing communications, for example) and laws, agreements or arrangements on mutual legal assistance (for rapid preservation of data, for example). In determining the strength of new legislation, States should be encouraged to be inspired by the provisions of the Council of Europe Convention on Cybercrime;

(d) Governments, the private sector and non-governmental organizations should work together to bridge the digital divide, to raise public awareness about the risks of cybercrime and introduce appropriate countermeasures and to enhance the capacity of criminal justice professionals, including law enforcement personnel, prosecutors and judges. For this purpose, national judicial administrations and institutions of legal learning should include comprehensive curricula on computer-related crime in their teaching schedules;

(e) The Eleventh Congress should devote considerable attention to establishing, improving and broadening the current practical tools for international information-sharing, early warning and response mechanisms, damage-limitation measures in the fight against cybercrime (using Interpol, 24/7 alert mechanisms of the Group of Eight, the Convention on Cybercrime, Computer Emergency Response Teams (CERTs) and Forum of Incident Response and Security Teams (FIRST)), which are still limited to some countries, mostly developed ones. These tools should be made available internationally in order to share knowledge and information concerning ways and means of recognizing, protecting, avoiding and handling new types of cybercrime and to inform the public of effective response mechanisms. In addition, special emphasis should be given to making these practical tools available to developing countries and offering related training;

(f) Cybercrime policy should be evidence-based and subject to rigorous evaluation to ensure efficiency and effectiveness. Therefore, concerted and coordinated efforts at the international level should be made to establish funding mechanisms to facilitate practical research and curb many types of newly emerging cybercrime. It is, however, equally important to ensure that research be internationally coordinated and that research results be made widely available;

(g) UNODC should bring the results of the Workshop on Measures to Combat Computer-related Crime, to be held during the Eleventh Congress, to the attention of the second phase of the World Summit on the Information Society, to be held in Tunis in 2005, for its consideration.

Notes

[1] D. B. Parker, S. Nycum and S. S. Oüra, *Computer Abuse* (Menlo Park, California, Stanford Research Institute, 1973).

[2] Donn B. Parker, *Computer Crime: Criminal Justice Research Manual* (Washington, D.C., United States Department of Justice, 1979).

[3] Donn B. Parker, *Computer Crime: Criminal Justice Research Manual* (Washington, D.C., United States Department of Justice, 1989).

[4] Russell G. Smith, Peter N. Grabosky and Gregor F. Urbas, *Cyber Criminals on Trial* (Cambridge, Cambridge University Press, 2004).

[5] Council of Europe, *European Treaty Series*, No. 185.

[6] In some countries, where wireless LANs have been adopted by residential Internet users, unsecured LANs have been used to gain unauthorized access to the Internet for a variety of purposes. This is often associated with “war driving” (using a laptop computer in an automobile to locate and log wireless access points or “hotspots”).

[7] In some countries, the concept of “theft” refers only to tangible goods and involves depriving a person of a tangible thing; hence, it does not extend to theft of an intangible good and it would not cover making a copy of a digital file. Some countries do not address such actions through criminal or penal sanctions but instead regard this as covered by civil law, including copyright regimes.

[8] Bram Cohen’s BitTorrent peer-to-peer software is increasingly being used to share large data files for both legitimate purposes (such as distribution of open source software, computer games or “peer-casting” of television programming) and by video pirates. For an overview of video piracy, see Clive Thompson, “The Bit Torrent effect”, *Wired*, 13 January 2005; and Jeff Howe, “The shadow Internet”, *Wired*, 13 January 2005.

[9] *IC3 2003 Internet Fraud Report*: *January 1, 2003-December 31, 2003* (National White Collar Crime Center and Federal Bureau of Investigation of the United States).

[10] See Michael D. Mehta, Don Best and Nancy Poon, “Peer-to-peer sharing on the Internet: an analysis of how Gnutella networks are used to distribute pornographic material”. *Canadian Journal of Law and Technology*, vol. 1, No. 1 (January 2002); and United States of America, General Accounting Office, *File Sharing Programs: Peer-to-peer Networks Provide Ready Access to Child Pornography*, GAO-03-351 (Washington, D.C., February 2003).

[11] Dick Thornburgh and Herbert S. Lin, eds., *Youth, Pornography and the Internet* (Washington, D.C., National Academy Press, 2003).

[12] For an overview of laws in 24 countries addressing racist, xenophobic and anti-Semitic material, see the document on the subject that was considered by the Organization for Security and Cooperation in Europe Conference on Anti-Semitism (CIO.GAL/25/04/Rev.1), held in Berlin from 28 to 29 April 2004.

[13] Scott Berinato, “The truth about cyberterrorism”, *CIO Magazine*, 15 March 2002.

[14] On commercially available products that use quantum cryptography to encrypt data over optical-fiber-based systems or wireless networks see Gary Stix, “Best-kept secrets”, *Scientific American*, January 2005.

[15] For an analysis of the information and communication technology aspects of the Millennium Development Goals, see International Telecommunication Union, *World Telecommunication Development Report 2003: Access Indicators for the Information Society*, 7th ed. (2003). The study provides an interesting assessment of the millennium development goals relevant to information and communication technologies; the new Digital Access Index (DAI) looks particularly promising.

[16] China Internet Network Information Center, *15th Statistical Survey Report on the Internet Development in China (Jan. 2005)* (www.cnnic.net.cn) (accessed on 25 January 2005).

[17] Internet Systems Consortium (http://www.isc.org).

[18] Derived from International Telecommunication Union, *World Telecommunication Indicators Database*, 8th ed. (2004).

[19] *World Economic and Social Survey 2000* (United Nations publication, Sales No. E.00.II.C.1).

[20] For a statistical analysis of the complexity of the digital divide, see the conceptual framework put forward in George Sciadas, ed., *Monitoring the Digital Divide ... and Beyond* (2003).

[21] It has been noted that ironically these circumstances recreate on a different level a digital divide at precisely the juncture where it was about to be bridged and may lead to undermining local business confidence or the incipient attractiveness for investment.

[22] The primary difference between an anonymous service and a pseudonymous service is that a pseudonymous service preserves an identity (an alias or “nym”) over a certain period of time (and consequently, there may be a stronger link between the pseudonymous identity, the subscriber identity and the “real-world” identity). An anonymous service, in its purest form, is essentially a one-shot or single-transaction service. There are various kinds of anonymous and pseudonymous services, most providing proxies, chains or mix-nets to access one or more typical Internet services such as e-mail remailers, Web surfing, IRC or Usenet newsgroups. There are also degrees of anonymity and pseudonymity, depending not simply on factors such as the underlying encryption and authentication software but also on the nature and security of the anonymizing server or network of servers, the “nym” creation procedures and, in the case of pay services, the billing mechanism.

[23] David H. Crocker, rev., *Standard for the Format of ARPA Internet Text Messages*, RFC 822 (13 August 1982).

[24] In the data retention workshop held during the Group of Eight Government/Industry Dialogue on Safety and Confidence in Cyberspace in Berlin in October 2000, the following cost implications for data retention were identified: log storage volumes; retrieval of relevant data; engineering and development; administrative, operational and training costs; providing security and privacy; liability in handling for and delivery to law enforcement; and costs associated with opportunity and customer trust.

[25] Data may be held by service providers for varying lengths of time, depending upon business models, services and technologies. Some data is held for billing purposes, other data is held for

system performance auditing. Time frames vary from a few seconds to longer periods that may be required or allowed, for purposes other than law enforcement, by their national legislation. Different types of traffic data are also held for different periods of time; for example, network access logs (RADIUS or the Terminal Access Controller Access Control System (TACACS+)) have different business and data storage requirements than NNTP logs and, as a result, may, in certain circumstances, be available for longer periods. Content is not typically retained or available.

[26] *Recommendations for Tracing Networked Communications across National Borders in Terrorist and Criminal Investigations* (http://canada.justice.gc.ca/en/news/g8/doc2.html).

[27] See *CERT Coordination Center, 2003 Annual Report* (www.cert.org); and Forum of Incident Response and Security Teams (www.first.org).

[28] Ulrich Sieber, *Legal Aspects of Computer-Related Crime in the Information Society: COMCRIME Study* (1 January 1998).

[29] Sieber's model of six waves of national legislation has been applied to the Australian experience in Russell G. Smith, Peter N. Grabosky and Gregor F. Urbas, *Cyber Criminals on Trial* (Cambridge, Cambridge University Press, 2004).

[30] Organization for Economic Development and Cooperation, *Computer-Related Crime: Analysis of Legal Policy*, ICCP Series, No. 10 (1986); see also recommendation No. R (89) 9, adopted by the Committee of Ministers of the Council of Europe on 13 September 1989.

[31] Country report for China, provided for the Asia-Pacific Conference on Cybercrime and Information Security organized in Seoul from 11 to 13 November 2002 by the Economic and Social Commission for Asia and the Pacific and the Ministry of Information and Communication of the Republic of Korea. The number of offenders may be large given that, in one Beijing district (Haidian District Procuratorate), 52 suspects were arrested between 2001 and May 2004, 48.4 per cent of them for hacking.

[32] Council of Europe, *European Treaty Series*, No. 185.

[33] *International Review of Criminal Policy*, Nos. 43 and 44 (United Nations publication, Sales No. E.94.IV.5).

[34] The Regulation of Investigatory Powers Act 2000 of the United Kingdom brings forward a definition of traffic data in article 2.9, although that definition also includes subscriber information. There is a conception of traffic data contained in the United States definitions of "pen register" and "trap and trace device" (United States Code, title 18, sect. 3127) that was updated through the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (PATRIOT) Act of 2001.

[35] With respect to subscriber information, in some countries there may already be existing regulations in the sphere of telephony (customer, name and address information).

[36] Relevant international instruments include, for example, the Council of Europe's 1981 Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data (Council of Europe, *European Treaty Series*, No. 108) or the 1980 Organization for Economic Cooperation and Development (OECD) Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data. Those sought to establish principles according to which personal information must be obtained fairly; used only for the original specified purpose; adequate, relevant and not excessive to that purpose; accurate and up to date; accessible to the subject; kept secure; and destroyed after its purpose is completed. The degree of obligation was further strengthened in some jurisdictions, for example, by the data protection directives of the European Parliament and the Council of the European Union (directive 95/46/EC and directive 97/66/EC). Following from those, numerous European countries have implemented stronger data protection laws to comply with their legal obligations to meet the standards of the directives. Outside of Europe, there are also instruments with

similar provisions for dealing with personal data, such as the Personal Information Protection and Electronic Documents Act of Canada.

[37] Note that “data preservation” ensures the existing specified information in relation to a particular subscriber is not deleted. By contrast, “data retention” is a general requirement that is designed to compel all Internet service providers to collect and retain a range of data concerning all subscribers.

[38] Roderic Broadhurst, “Content crimes: criminality and censorship in Asia”, paper presented at Octopus Interface: the Challenge of Cybercrime, Strasbourg, France, 15-17 September 2004.

[39] Council of Europe, *European Treaty Series*, No. 189.

[40] The model law can be found on the web pages of the Legal and Constitutional Affairs Division of the Commonwealth Secretariat (http://www.thecommonwealth.org/shared_asp_files/uploadedfiles/{DA109CD2-5204-4FAB-AA77-86970A639B05}_Computer%20Crime.pdf).

[41] During the Eighth Congress, a workshop on computerization of the administration of criminal justice was held (A/CONF.144/14). Already in 1992, the Organization produced the *Guide to Computerization of Information Systems in Criminal Justice* (United Nations publication, Sales No. E.92.XVII.6). During the Ninth United Nations Congress on the Prevention of Crime and the Treatment of Offenders, in 1995, workshop on international cooperation and assistance in the management of the criminal justice system: computerization of criminal justice operations and the development, analysis and policy use of criminal justice information was held (A/CONF.169/13) (see also Asia and Far East Institute for the Prevention of Crime and the Treatment of Offenders, *The Global Challenge of High-Tech Crime: Workshop on Crimes related to the Computer Network; Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders, 15 April 2000, Vienna, Austria* (Tokyo, April 2001)).

[42] *International Review of Criminal Policy*, Nos. 43 and 44 (United Nations publication, Sales No. E.94.IV.5).

[43] See the background paper for the workshop on crimes related to the computer network (A/CONF.187/10).

[44] Peter Grabosky and Roderic Broadhurst, “The future of cyber-crime in Asia”, *Cybercrime: the Challenge in Asia*, Roderic Broadhurst and Peter Grabosky, eds. (Hong Kong University Press, 2005), pp. 347-360.

[45] See “G8 Berlin Meeting: Government/Industry Dialogue on Safety and Confidence in Cyberspace (Summary and Assessment)” (available at http://www.mofa.go.jp/policy/economy/summit/2000/lyon.html); and Kuriko Miyake, “G8 concludes Tokyo high-tech crime meeting” (available at http://archives.cnn.com/2001/TECH/internet/05/31/g8.cyber.crime.idg).