Crime Law Soc Change (2007) 47:201–223
DOI 10.1007/s10611-007-9069-1

Requirements of prosecution services to deal with cyber crime

Peter Grabosky

Published online: 13 October 2007

Abstract The advent of digital technology and the convergence of computing and communications have begun to change the way we live. These trends have also created unprecedented opportunities for crime. Criminal activities that were not foreseeable two decades ago have become facts of life today. Digital technologies now provide ordinary citizens, even juveniles, with the capacity to inflict massive harm. It is essential for public prosecutors to equip themselves with the knowledge that will permit an effective response. The continued uptake of digital technology will create new opportunities for criminal exploitation.

Introduction

The advent of digital technology and the convergence of computing and communications have begun to change the way we live. These trends have also created unprecedented opportunities for crime. Criminal activities that were not foreseeable two decades ago have become facts of life today. Digital technologies now provide ordinary citizens, even juveniles, with the capacity to inflict massive harm. As never before, and at negligible cost to themselves, lone offenders can inflict catastrophic loss or damage on individuals, companies, and governments from the other side of the world. The continued uptake of digital technology will create new opportunities for criminal exploitation.

We are all familiar with the term "digital divide." The uptake and penetration of digital technology is quite uneven around the world. What is new in a highly "wired" country may not yet appear on the "radar screen" of a country that has just entered the digital age. But even these countries may unwittingly serve as havens for computer criminals. Today, most nations are vulnerable to computer-related crime. Sooner or later all will be. It is therefore important to establish the necessary legal (substantive and procedural) and institutional framework enabling prosecutions of these new and emerging forms of crime. It is essential for public prosecutors to equip themselves with the knowledge that will permit an effective response. The following pages are intended to provide a roadmap for such a response, and to identify some of the key issues that prosecutors should bear in mind as they enter the digital age.

This paper was commissioned by the Organizing Committee and written by Professor Peter Grabosky, BA, MA, PhD, FASSA, Australian National University.

P. Grabosky (✉)
Australian National University, Canberra ACT 0200, Australia
e-mail: peter.grabosky@anu.edu.au

Conceptualization of cyber crime

This paper uses the terms cyber crime and computer-related crime interchangeably. Cyber crime takes three general forms:

(a) Crimes where the computer is used as the *instrument* of crime (as in the production and dissemination of child pornography);
(b) Crimes where the computer is the *target* of crime (as in a denial of service attack); and
(c) Crimes where the computer is *incidental* to the offence (such as communications in furtherance of criminal conspiracies, or the use of computers in maintaining records of criminal transactions such as drug dealing).

Box 1: Cyber crime terms

Hacking: Obtaining unauthorized access to a computer.
Distributed Denial of Service Attack: An individual (usually a hacker) gains remote access to a number of computers and directs them against a target (usually a computer system belonging to a government or large commercial entity). By overloading the target computer, the attack will impede legitimate access and may render the system inoperable.
Spam: Unsolicited electronic mail, often transmitted in large volume, whether for legitimate commercial purposes or in furtherance of fraud.
Phishing: Transmitting a form of Spam containing links to Web pages that are designed to appear to be legitimate commercial sites. They seek to fool users into submitting personal, financial or password data. Clicking on the link may also lead to infection of one's computer by a virus, or may allow access to one's computer by a hacker (Krone 2005).
Virus: A computer program that may spread from computer to computer, as files containing the program are opened, using up available memory and degrading the "infected" systems and their networked computers.
Worm: A computer program that reproduces itself and spreads through a network, using up available memory. It differs from a virus in that it does not require human intervention (such as the opening of a file) in order to spread.
Malicious Code: Computer programs designed to cause damage to a computer or system; worms or viruses.
Trojan Horse: a malicious program disguised as legitimate software but which, when transmitted to an unsuspecting recipient, may impede functioning of the target computer system, and may even facilitate unauthorized access and control over one's computer.
"Bot" (abbreviation of robot): a computer program that runs automatically. Some bots have beneficial uses, but others may be employed to gain unauthorised control over a target's computer.
Encryption: The process of mathematically transforming digital information so that it is unintelligible to anyone other than a person in possession of an algorithm or "key" that will permit the data to be converted to its original state

One might also distinguish between *new crimes, which use new technologies*, e.g. distributed denial of service attacks and hacking (these are the offences which came about due to the introduction of Internet technologies) and *old crimes using new technologies*, e.g. banking fraud (these are the offences which have already occurred, but they are now being

perpetrated in new ways). The rapid takeup of digital technology around the developed world suggests that digital or electronic evidence will be present at many, if not most, ordinary crime scenes, in the form of mobile telephones or digital diaries.

Every new *application* of digital technology is subject to criminal exploitation. The greater the volume of commerce, entertainment and communications that occur on-line, the more opportunities there are for criminals. The brief history of digital technology to date abounds with examples:

- Ordinary criminals and international terrorists now communicate with greater efficiency than ever before, using wireless technology and encryption.
- Digital technology permits perfect reproduction and instantaneous communication of text, images, video, sound, and multimedia combinations. Piracy is commonplace. So too is the collection and dissemination of child pornography.
- Credit card details and other personal information are stolen and used for a variety of criminal purposes.
- Electronic funds transfers have been intercepted and/or diverted by criminals.
- The establishment of on-line auctions was quickly welcomed by individuals who sought to avoid paying for products that they had purchased, or to avoid delivery of the products that they had purported to offer for sale.
- The advent of chatrooms frequented by children also attracted adults seeking to lure children into illicit relationships.
- On-line share trading has inspired some to attempt to manipulate the price of a stock by engineering a pattern of transactions to attract the attention of the unwitting investor to create the illusion of momentum in share trading.
- Individuals now transmit fraudulent investment solicitations instantaneously, to millions of people, at negligible cost.

Box 2: Extortion in the Digital Age

Extortion is where a person obtains something of value from another by threatening harm to his person, reputation, or property. Digital technology may be applied to extortion in numerous ways (Grabosky, Smith and Dempsey 2001, Ch. 3).

The internet can be used as the medium by which a threat is communicated.

The victim's information systems may be the target of the extortion threat.

Where the offence entails blackmail, the Internet may be the medium through which the offensive information is communicated.

Electronic funds transfer may be used as a means of effecting an extortion payment.

The Internet and World Wide Web may be used to obtain personal information that may identify or be used against prospective victims.

http://computercops.biz/article4091.html (visited 13 March 2005)

Manipulation of financial markets

Most countries have stock markets. Increasingly, ordinary investors are able to buy and sell shares on-line without dealing through intermediaries such as underwriters, brokers, and investment advisers. The convenience of online share trading is such that will be introduced in newly capitalist societies and transitional economies in the fullness of time. While this may enhance the efficiency of securities markets, it also provides opportunities for criminal exploitation. Meanwhile, these countries may expect to encounter some of the same difficulties that the United States and other Western countries faced in the 1990s. The fundamental criminality is still reducible to the basics: misrepresenting the underlying value of a security at the time of the initial public offering, or market manipulation during secondary trading of a security, through the dissemination of false information, or by engineering a deceptive pattern of transactions to attract the attention of the unwitting investor [10], Ch. 6).

Common practices that may be expected to re-appear in "newly wired" countries include

- The use of the Internet and World Wide Web to spread false tips or rumours about a particular company and its shares. This would include spamming, infiltration of chatrooms, and counterfeiting of websites for the purpose of introducing price-sensitive information.
- The use of multiple aliases and coordinated trading to create momentum in a company's share price.

Industrial espionage

In the competitive global economy of the 21st century, obtaining a competitor's trade secrets and other economic information of a sensitive nature can be extremely lucrative. Depending on the methods employed, it can also be illegal [15]. Traditional espionage techniques are now complemented by high tech methods. Given that much, if not most, information today exists in digital form, industrial espionage has begun to have its digital manifestations. Web-based research through open sources may be legitimate. But the insertion of a Trojan horse or backdoor into a competitor's computer network is quite another matter.[1] The vulnerability of wireless technology and Internet telephony to industrial espionage goes without saying.

Cyberterrorism

One of the more prominent issues of our time is the threat of terrorism. The term "cyber terrorism" has been used rather loosely to refer to the application of digital technology to terrorist activity. One way of conceptualizing cyberterrorism is Denning's [7], 10): "unlawful attacks against computers, networks and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives".

For some years now, thoughtful people in industrialized societies have been alert to the threat of attacks against what we call *critical infrastructure*. In other words, communications, electric power, air traffic control and financial systems all depend on software and are vulnerable to disruption. The annals of cybercrime contain examples of successful attacks against air traffic control systems, sewage treatment facilities, and large electronic retailers,

[1] http://www.computerweekly.com/Articles/2005/06/07/210245/trojan-spyware-suspects-arrested-as-major-industrial-espionage-scandal.htm (visited 17 August 2007).

as well as the occasional mail bombing of government servers and defacement of government websites. But none of these meet Denning's definition.

Although the "electronic Pearl Harbor" scenario may be remote, there are a number of ways in which digital technology may be used in furtherance of, or complementary to, terrorist activity. Digital technology of course may be used for the remote detonation of explosive devices. And while Denning may be correct in asserting that terrorists continue to prefer truck bombs to logic bombs, the use of a cyber attack to complement or enhance a terrestrial attack should not be discounted. Imagine if an attack on the scale of 9/11 were accompanied by a takedown of the telephone and electric power systems in the target metropolitan area.

Technology as a means to facilitate terrorism

Of course, digital technology can enhance the efficiency of any organization, legitimate or otherwise, that makes use of it. For example, it lends itself nicely to the following terrorist applications [22]:

Intelligence

Terrorists may seek to acquire open source intelligence on an adversary, or collect classified information by hacking into the adversary's computer systems.

Communications

Terrorist groups may send and receive messages, often concealing their content through encryption and steganography (concealing messages within images). The nature of the Internet and World Wide Web are ideally suited to communications across widely dispersed elements of a network.

Propaganda

Terrorist groups may communicate directly to a general worldwide audience, or to specialist target audiences, bypassing journalistic editing and government censorship. This may include inflammatory hate speech intended to legitimize violence against specified adversaries.

Psychological warfare

The Internet may be used as a means of tactical deception by terrorist organizations. By generating anomalous patterns of traffic they can give the erroneous impression that an operation may be imminent. The fabrication of "chatter" may distract law enforcement and intelligence services from true terrorist activity.

Another form of psychological warfare can involve general or specific threats or displays of force. Webcasts of hostages, and even hostage executions, can reach the world. These may be coupled with threats against nationals of specific countries who may be identified with causes anathema to the terrorist organization.

Recruitment and fund raising

The cities of the world house many young unemployed, marginalized and resentful people. Some of them may well be attracted to militant causes, and terrorist groups may use the

Internet and World Wide Web to actively recruit new members. Such groups may raise funds through charity and other front organizations, and digital technology facilitates funds transfers to launder money and/or to finance terrorist operations.

Training

Terrorist groups may use the Internet and the Web for instructional purposes, to teach attack techniques and skills. For example, an English translation of an Al Qaeda Training Manual reported to have been found on a computer file in Manchester, England [5] is posted on the website of the US Department of Justice.[2]

The above discussion of various types of cybercrime is by no means exhaustive. It does illustrate the range of issues that governments have to deal with. Legislatures will be called upon to draft laws that prohibit harmful activity in cyberspace, but which do not discourage legitimate use of digital technology, on which societies and economies will increasingly depend. Prosecutors will be confronted with hard choices about what cases to bring, how to match existing law with the behaviour in question, and how to present their cases in court.

The prosecutor's role

The extent of the prosecutor's involvement with cybercrime will vary from one country to another depending upon the prosecutor's role in the criminal justice system and on constitutional issues more generally. In civil law countries, the decision to begin an investigation may rest with the prosecutor, depending on whether coercive measures are necessary or special proceedings are required. Japanese prosecutors routinely direct investigations [11]. Prosecutors also play a central investigative role in Korea and China [23]. In the United States, especially at the Federal level, prosecutors are involved well 'upstream' of the criminal charge, and are often engaged in the planning, organization and execution of criminal investigations. This early involvement tends to arise from constitutional restraints on criminal investigation. These safeguards invite detailed and exacting prosecutorial oversight. In some countries, prosecutors will play an active role in policy development and in the drafting of legislation. Prosecutors may also become involved in the determination of a sentence following conviction.

In Northern Ireland, prosecutors have traditionally been relatively 'passive' recipients of evidence collected and presented to them by police. This reflects the British tradition of prosecutorial independence, which favors a degree of insulation from the police or from executive government. This relatively passive role also characterizes nations that have been influenced by British legal traditions such as India, Malaysia, and Singapore [23]. In Australia and the United Kingdom, the tradition of prosecutorial passivity is slightly tempered by the occasional practice of offering advice early in the course of an investigation, but only in serious or complex cases or where unusual legal issues were involved.

There are two particular benefits of prosecutorial involvement early in an investigation. First, prosecutors, given their awareness of the nature and quantity of evidence necessary to obtain a conviction, are in a position to ensure the efficiency and the effectiveness of the investigative process. Second, they are in a position to oversee the integrity of the investigative process, to ensure that the human rights of suspects are not violated. Of

[2] http://www.usdoj.gov/ag/manualpart1_1.pdf (visited 17 August 2007)

course, overzealous prosecutors may fail to perform either of these functions. But the best prosecutors will embody efficiency, effectiveness and justice.

Policy priorities

In some places, matters will take on a higher priority depending on economic or political developments. One of the most compelling illustrations of this is the current status of offences relating to Internet child pornography in the criminal justice systems of many nations. Heightening concerns about sexual exploitation of children in the 1990s happened to coincide with the growth in telecommunications and computing technology. These technological developments served greatly to facilitate the production, reproduction and dissemination of child pornography. Additional developments such as the widespread availability of strong encryption have further assisted in concealing this activity from the attention of law enforcement or other adversary interests.

Given the technological, legal and cultural diversity of the world's nations, it is not surprising that priorities differ. Some nations are deeply concerned about theft of intellectual property; for others, blasphemous or seditious communications are of paramount concern. Others still are concerned about the application of digital technology for the sexual exploitation of children.

The decision to prosecute

Faced with workload pressures, prosecutors in common law jurisdictions often must decide what cases they take on or not. In other legal systems, they may be required to prosecute once sufficient evidence is at hand.

In many modern jurisdictions, the principles by which discretionary decisions are reached are set out formally in a prosecution policy.[3] In others, law dictates the decision. Where discretion is allowed, the prosecutor's decision is essentially determined by two factors: the seriousness of the offence and the sufficiency of the evidence. The first of these is fairly objective; the available sentence will give some relative indication of the gravity with which an offence is regarded. Given the resource constraints under which most prosecutors labour, a case that is unlikely to result in any significant punishment may not be taken up. Sufficiency of evidence may entail more of a judgment call, although experienced prosecutors will be able to assess the probability of conviction with a fair degree of accuracy.

Looming over the decision to prosecute is the question of resources. The funds available to the prosecution service, or to an individual prosecutor's office, are usually limited. The threshold of what constitutes an acceptable case will vary, depending on how much is left in the year's budget. This is especially relevant in cases where the offender, or the evidence, is situated in another jurisdiction. For example, the cost of bringing an Internet Service Provider from France to testify in an Australian court is not trivial. A prosecutor's office can quickly use up its budget in pursuit of transnational cybercrime [3].

In some jurisdictions, other considerations that bear upon the decision to prosecute include the impact that the offence has had on society, the deterrent or educative potential of a successful

[3] Australia: *The Prosecution Policy of the Commonwealth* http://www.cdpp.gov.au/cdpp/prospol.html. United States: Principles of Federal Prosecution http://www.usdoj.gov/usao/eousa/foia_reading_room/usam/title9/27mcrm.htm. United Kingdom: *Code for Crown Prosecutors* http://www.cps.gov.uk/publications/docs/code2004english.pdf. People's Republic of China (Hong Kong Special Administrative Region): *Statement of Prosecution Policy and Practice* http://www.doj.gov.hk/eng/public/pub20021031toc.htm

conviction, and whether any special factors might militate in favour of or against prosecution. For example, all else being equal, the public interest might militate against prosecution of a terminally ill grandmother, but in favour of pursuing a notorious repeat offender.

In essence, prosecutorial decisions are determined by criminal justice policies based on a variety of criteria such as national values and interests, the social and economic impact of the offence, etc.

Presentation of evidence in court

In common law systems, prosecutors will bear primary responsibility for presenting evidence in court. Elsewhere, their role may be that of assisting a judge in fact finding. In cybercrime cases, this has often been a particularly important function, especially when judges and jurors are relatively unfamiliar with digital technology and its criminal misuse.

Sentencing

Prosecutors in many jurisdictions may also make recommendations regarding the appropriate sentence to impose on a convicted offender. In some countries, prosecutors devote a great deal of time to researching what similarly situated offenders have received, so that they may make an appropriate recommendation in the case immediately before them.

Substantive criminal law

Availability of law

The principle of *nullum crimen sine lege* is fundamental to most legal systems. Under this principle, behaviour, no matter how harmful, cannot be prosecuted unless it is formally prohibited by law. The person who released the I LOVE YOU virus in May 2000, for example, could not be prosecuted in the Philippines because there was no law in that country at the time that prohibited the release of malicious code. The history of criminal law in many countries is replete with examples of new offences that were created to cope with new forms of undesirable behaviour. The advent of digital technology has necessitated a great deal of legislative activity to this end. Indeed, very soon after the release of the I LOVE YOU virus, the Government of the Philippines introduced legislation to criminalize virus dissemination.

Certain forms of computer related crime are entirely new and require explicit legal prohibition. In the contemporary technological environment, the substantive criminal law would prohibit the following acts:

- *Unauthorized access to a computer system*. This would embrace hacking, often the first step in a chain of criminal activities.
- *Unauthorized destruction or modification of data*.
- *Impeding or interfering with the lawful use of a computer.* This would prohibit such activities as distributed denial of service attacks, and the release of viruses and worms.
- *Unauthorized interception of computer-mediated communications*

As we observed, computers may be used to commit a vast array of more conventional crimes, including, but not limited to, many varieties of fraud, forgery, the dissemination of child pornography, and copyright infringement.

The generality and flexibility of a country's traditional criminal law will determine whether or not it is able to embrace conventional crimes committed with digital technology. For example, at common law, the crime of theft required that an object be physically moved, with the intention of permanently depriving the owner of that object. Today, digital technology allows perfect reproduction of text, images, sound, video, and multimedia combinations. It is possible to steal trade secrets or to reproduce motion pictures by copying them, and leaving the originals in place. The fact that property may exist in intangible form has brought about a broadening in the law of theft, as well as criminal damage.

Box 3: Damage to intangible property
The accused had gained unauthorized access to a computer network and altered data contained on discs in the system. He was charged with damaging property under the United Kingdom's *Criminal Damage Act* 1971; The Act required proof of damage to tangible property. The prosecution succeeded in its claim that the discs and the 'magnetic particles' that they contained were one entity, and by altering the state of the magnetic particles, the discs themselves were damaged. The accused was convicted at trial, and appealed. The appeals court affirmed the conviction, holding that it was sufficient to prove that tangible property had been damaged, not that the damage itself was tangible. Damage was defined broadly to embrace the 'temporary impairment of value or usefulness.' Subsequent legislation, the *Computer Misuse Act* 1990, would make future prosecutions less problematic. (Rv Whiteley[1991] 93 Cr App R 25)

It has often been said that technology advances faster than the law. Where a particular act appears not to be covered by the existing legal prohibition, or where the law is poorly drafted, the prosecution may have no choice but to 'force' the facts into a form apparently consistent with the statute. In the I LOVE YOU case, prosecutors sought to charge the accused with the offence of using a computer to obtain credit card or other personal information for a fraudulent purpose. This was not even close to what the accused actually did (release the virus), and the inappropriate charges were eventually dropped.

By contrast, prosecutors in the United Kingdom were more successful with a prosecution under the Protection of Children Act 1978 when they charged the defendant with possessing indecent photographs. The defence maintained that data in digital form did not constitute a photograph. The court found that the data were a photograph 'in a different form.' Subsequent amendments to the Protection of Children Act sought to pre-empt future similar challenges, by referring to data 'capable of conversion into a pseudo-photograph' (Rv Fellows and Arnold [1997] 1 Cr App R 244). This case illustrates that legislation should be general enough to embrace technological developments, but not so general as to be impossibly vague. The use of technology-neutral language is ideal.

The application of digital technology to child pornography has understandably attracted the attention of legislators, law enforcement officers and prosecutors throughout the world. In terms of drafting legislation to criminalize child pornography in digital form, one encounters a number of hurdles. Not least of these are:

a. What constitutes pornography? What type of behaviour is being depicted? The narrowest definition would embrace only depictions of children engaged in explicit sexual activity. One could, however, imagine suggestive depictions of children entailing other than sexually explicit behaviour. To some observers, there is a significant difference between pornography and erotica; to others, not.

b. What constitutes a child? The legal age of consent for consensual sexual activity varies significantly around the world, as does the age of consent for participation in depictions of sexual conduct. Children's physical characteristics also differ significantly. Definitions of prohibited material may be based on the actual age of the person in the depiction, or on the person's apparent age. Moreover, child pornography may be produced without the involvement of children, or indeed, of any other person. Digital images may be enhanced or altered in a manner that give the appearance of child subjects. In reality, the image may be created *ex nihilo* (as is the case with cartoons) or transformed by technical means (the colloquial term for this is "morphing").
c. What constitutes possession? In common law jurisdictions, the essence of possession is (a) control, and (b) knowledge. In the United Kingdom, a university lecturer was prosecuted under s.160 of the Criminal Justice Act 1988 for possessing indecent images of children. The defendant maintained that he had browsed the Web and had visited some extreme sites out of morbid curiosity, but denied having downloaded any illegal content. Unbeknown to the defendant, the caching function of the Netscape browser software had evidently captured the images in question. Sites visited by mistake or through a misleading link could have achieved the same result. In any event, the defendant denied that he knowingly possessed the images in question. The court held that the 'offence of possession under section 160 is not committed unless the defendant knows he has photographs in his possession'. In some cases, the task of the prosecutor is made easier by the defendant's behaviour. It is easier to rebut such a defense when forensic examination of the computer reveals that the file in question had been downloaded repeatedly over a period of time. Some unwitting offenders do not know that data, once deleted, may be recovered by forensic computing specialists. This may also constitute evidence of possession.

Box 4: Possession, Knowledge and Control

An individual's computer was found to be storing some 27,000 images, a significant number of which entailed child pornography. The accused maintained that he had accidentally run across the offending images, which were then automatically cached on his hard drive. Arguing that he did not want the images to be saved on his hard drive, he had manually deleted the images by dragging them to his computer's recycle bin. He claimed that the images were not stored, but saved against his will, and only temporarily displayed. The government was able to prove that manual deletion of the files represented control over them, and that the images would not have been stored had the accused not 'volitionally reached out' for them. The fact that he had asked the operator of one website 'to be given access to pictures of 'naked young girls'' and that he had purposefully visited websites containing child pornography, suggested that his possession was knowing. United States v Tucker 150 F Supp 2d 1263 (D Utah 2001) 305 F 3d 1193 (10th Cir, 2002).

As the above discussion suggests, the substantive criminal law must not be drafted or applied indiscriminately. Legislation that is overbroad or vague may be subject to inappropriate application. It may be seen as an invitation to the abuse of power. The legitimate goal of criminalizing communications in furtherance of terrorist conspiracies does not justify legislation that would also prohibit or discourage legitimate political expression. In order to avoid this problem, care must be taken to formulate laws as precise and specific as possible.

Criminal procedure law

The search of a person's home or workplace, and the seizure of one's property are among the most formidable powers that the state may wield against a citizen. Accordingly, it is essential that these powers be wielded in accordance with the rule of law. Most countries require that their law enforcement agents obtain some form of judicial authority (in the form of a search warrant) before searching for and seizing private property. In other countries, however, this authority may be vested in prosecutors or police [8], 205).

Ideally, information required in order to obtain a search warrant will be very detailed and specific. A formal request for a warrant should provide probable cause that a crime has been committed, and should identify with considerable specificity what evidence is to be sought. The actual search should be within the scope of the warrant [2].

Details required for a warrant vary depending on the location of the computer and the intrusiveness of the proposed search. Warrants conferring authority to intercept telecommunications (including email in transit) can be the most exacting. Warrants authorizing surreptitious entry (sometimes referred to as 'sneak and peek') may also require more details than a warrant for an 'ordinary' search. Access to a computer in a suspect's possession may require a search warrant. By contrast, a suspect's stored email (but not email in transit) can be obtained from a service provider by a subpoena. Basic customer or subscriber information (but not the content of messages) may be obtained from a carrier or service provider through a court order.

While the laws of some countries provide for general search warrants, others require great specificity regarding the premises to be searched, and the nature of the evidence sought[4]. In some countries, evidence obtained as a result of searches that exceed the scope of a warrant may be inadmissible in court. Prosecutors should therefore be concerned that warrants are sought, drafted, and executed properly, consistent with the rule of law.

Undercover investigations

People who use the Internet sometimes pretend to be someone other than who they really are. In some cases, this may entail harmless role playing. In other cases, it may be a means of fraud or espionage. Cybercrime investigators may also impersonate private citizens in the course of an investigation. They may also clandestinely obtain personal information. Today, the capacity of the state to violate the privacy of its citizens is unprecedented[5].

Law enforcement agencies have designed elaborate ruses to trap computer criminals. In a 1995 operation codenamed "Operation Cybersnare," the US Secret Service covertly established an Internet discussion group which served as a forum for the purchase of stolen cellular phone access numbers, credit card numbers and personal identity information. Criminals joining the group who offered illicit products for sale were identified and prosecuted.[6]

The practice of law enforcement officers posing online as children in order to trap adults in search of illicit assignations has occurred for over a decade, and is common in many

[4] Because of constitutional safeguards, the United States has particularly exacting constraints on search and seizure. See [24].

[5] Issues regarding the importance of rule of law are discussed in a separate paper and workshop of this Summit. See also below section on human rights.

[6] http://www.bbsdocumentary.com/library/CONTROVERSY/RAIDS/CYBERSNARE/ (visited 6 May 2005).

western democracies [19, 190]). Other countries do not permit online investigations, regarding them as an excessive use of police power. Undercover patrolling of the Internet can encroach upon personal privacy and can inhibit freedom of expression, not only of criminals but of innocent persons as well. A strong, vigorous society and a vibrant economy depend to a significant extent on these freedoms. For this reason, if online undercover investigations are to be allowed, they should be conducted in a manner subject to strict guidelines, and rigorous oversight.

Remote searches

The nature of digital technology has complicated the challenge of search and seizure. Evidentiary data may be dispersed across a computer network, in unknown places far removed from the physical location of a search, but still accessible through computers located on the search premises. The actual location of the data may well be in another jurisdiction or even another country. While authorities in some countries may not be concerned that their investigation is taking them electronically into another sovereign jurisdiction, authorities in that jurisdiction may be very concerned. This further complicates the problems of cross-national cyber crime and raises the importance of mutual legal assistance, to be discussed below.

Box 5: Remote searches in Australia

Under Australian federal law, search powers related to computer evidence are no longer confined to specific locations. The *Cybercrime Act 2001* (Cth) envisaged that evidentiary data may be dispersed across a computer network, and allows searches for off-site data accessible through computers located on the search premises. The term "data held in a computer" refers to "any data held in a storage device on a computer network of which the computer forms a part". There are no geographical limits specified, nor is there any requirement that consent be obtained from third parties. However, section 3LB of the *Crimes Act 1914* (Cth), inserted by the *Cybercrime Act*, requires the notification, where practicable, of the occupier of the remote premises. This can be more complicated than it sounds, because in the course of a search through a networked environment, one is not always certain "where one is." It is customary in Australia to advise foreign third parties after the fact that such a remote search has taken place.

Cryptography

The sophistication of cyber crime is compounded by the widespread availability of cryptography. Once the monopoly of military organizations and intelligence services, technologies for concealing the content of electronic communications from all but the intended recipient are now widely available. Encryption is ideally suited to those offenders who wish to communicate in furtherance of criminal conspiracies, or who wish to conceal information that might be used against them in court. These might include records of criminal transactions, or illicit images. In addition to cryptography and steganography, technologies enable individuals to conceal their identities on line, or to impersonate other users. These technologies make it very difficult to identify suspects [14]. A number of nations are moving towards compulsory disclosure of cryptographic keys subject to judicial oversight. Jurisdictions with constitutional protection against self-incrimination may deem it an aggravating circumstance or even a separate offence to use cryptography in furtherance of a crime.

Collecting, preserving, analyzing and presenting digital evidence

One of the most significant differences between cybercrime and terrestrial crime is the nature of evidence. There are differences in the form it takes, how it is stored, where it is located, how it is found, and in the physical limitations of what it will tell you. Digital evidence is intangible. It is often volatile. And it may also be massive in quantity, thereby posing substantial logistical challenges.

Nevertheless the basic principles remain the same for handling digital evidence as for physical evidence [13]. Ideally, examination of the evidence will entail no alteration or modification of the data. The original data would be preserved and copied; and any examination would be carried out on the copy. Any changes to the original, if necessary should be explicitly documented and justified, in order to minimize defence challenges to its integrity. In court, the evidence should be presented in a manner that does not change its meaning.

There are three basic issues arising from the use of electronic evidence. First, as discussed above, the defence may question the identity of the author of the evidence in question ('It wasn't me; it was somebody else.') Second, the defence can claim that the evidence was tampered with. Third, it can argue that the unreliability of computer programs created inaccuracies in the output.

Efforts to standardize forensic procedures have occurred on a number of fronts. The Computer Crime and Intellectual Property Section of the US Department of Justice developed Federal Guidelines for Searching and Seizing Computers in 1994. The guidelines have been revised and updated periodically since then, most recently in 2002 [24].

In March 1998, the International Organization on Computer Evidence was appointed to draw international principles for the procedures relating to digital evidence, to ensure the harmonization of methods and practices among nations and guarantee the ability to use digital evidence collected by one state in the courts of another state.[7]

Standardised forensic procedures have also been developed by the FBI's Computer Analysis Response Team. In the United States, courts have given their imprimatur to certain standardized forensic practices. In one recent case the courts summarized in great detail the procedures taken at each step by investigators, holding it out as a textbook example of best practice [211 F.R.D. 31 (D. Conn. 2002)]. In the United Kingdom, the Association of Chief Police Officers has drafted guidelines in relation to preferred forensic procedures.[8]

This developing standardization of forensic practice (assuming that investigators adhere to these standards) will give the defence less opportunity to challenge investigative techniques. Prosecutors should be aware that departures from recognized best practices, to the extent that they occur, are likely to be seized upon by defence counsel. The laws of evidence in a given jurisdiction should be able to accommodate the transformation of intangible evidence into a form intelligible to judges and juries.

Human rights safeguards

For all its benefits, digital technology can pose a grave threat to human freedom. The capacity of governments to undertake surveillance of their citizens, and the vast amounts of personal information that can be collected, stored, and analysed, can contribute to unprecedented abuses of power. For this reason, many governments take steps to safeguard the human rights of criminal suspects as well as law-abiding citizens.

[7] http://www.ioce.org/

[8] http://www.acpo.police.uk/asp/policies/Data/gpg_computer_based_evidence_v3.pdf

Legality is a basic principle of government. Investigation and prosecution of cybercrime, no less than other activities of the state, should be done according to rules. The reason for this is simple: The government sets an example for all its citizens. When the government breaks the law, the public will hold the government and the law in contempt. By breaking the law, the government invites the public to take the law into its own hands. It invites crime.

The investigation and prosecution of cybercrime risks the violation of some fundamental human rights. What are the general principles that might govern the state's response to cybercrime? First of all, there should be formal guidelines that spell out what methods may be undertaken under what circumstances. Prosecutors should regard themselves as guardians of these guidelines and of the rule of law generally. Ideally, the guidelines will be consistent with the following principles:

Prosecution should not be gratuitous. It should require reasonable suspicion of criminal activity. It should not be directed at relatively trivial matters, that is, minor crimes or mere technicalities. The techniques of investigation to be employed should entail the least intrusive means available. If other, less intrusive means of obtaining necessary evidence are available, they should be used instead.

Formal authorization should be required prior to commencing a criminal investigation. The stringency of standards for authorization and the degree of justification required, should be proportionate to the degree of intrusiveness that the investigation will entail.

In common law countries, for example, surveillance of public places can be done as a matter of routine. Access to stored data is more easily obtained, subject to subpoenas served on third parties, or ordinary search warrants served on the target premises. Telecommunications interception (that is, communications during the course of transmission) may only be undertaken subject to the most exacting guidelines, requiring prior approval by an independent judicial authority.

The importance of international cooperation to combat cyber crime will be discussed below. For present purposes, it is important to note that such cooperation is easier to achieve when there is fundamental consensus across nations regarding the methods and procedures of investigation and prosecution, and safeguards against abuses that may occur in the collection and use of evidence. To the extent that a nation's policies and practices are consistent with The Universal Declaration of Human Rights[9], the International Covenant on Civil and Political Rights[10], and the European Convention on Human Rights[11], international cooperation is more likely to be forthcoming.

International cooperation and mutual legal assistance

Cyber crime can be committed from the other side of the world as easily as from next door. Moreover, a single communication in furtherance of cyber crime can pass through many providers in different countries with different legal systems.

Digital footprints are fragile or ephemeral, so fast action is required. This is especially the case when one seeks to interdict a crime in progress, such as an electronic attack on critical infrastructure. It is also the case when one seeks to gather evidence relating to a crime that has been recently committed. The task becomes very difficult when an attack transits multiple

[9] http://www.un.org/Overview/rights.html (visited 8 May 2005)

[10] http://www.unhchr.ch/html/menu3/b/a_ccpr.htm (visited 8 May 2005)

[11] http://www.hri.org/docs/ECHR50.html (visited 17 August 2007)

jurisdictions with different regimes for preservation of evidence. Thus, traditional methods of law enforcement are 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. Even "local" crimes may have an international dimension, and assistance may be required from all countries through which an attack was routed.

If an apparent crime is indeed worth investigating, assistance may be needed from authorities in the country where the offence originated, and/or from authorities in the country or countries through which the offending activity may have transited on its way to the target, or where evidence of the crime may be situated. There are two basic elements to cooperation: informal investigator-to-investigator assistance, and formal mutual assistance.

Informal assistance can be more expeditious, and is the preferred method of approach where compulsory powers (i.e. search warrants or extradition) are not required. It is based on good working relationships between police services of the countries in question, born of contacts made over time in the course of conferences, courtesy visits, and previous joint investigations.

Formal mutual assistance, on the other hand, is a more cumbersome process traditionally invoked pursuant to treaty arrangements between the countries in question, and involving the exchange of formal documents. It almost always requires that the offence in question be over a certain threshold of severity, and be a crime in both the requesting and the requested countries. This latter convention is referred to as 'dual criminality'.

There exists a web of bilateral mutual assistance treaties between pairs of nations as well as multilateral agreements such as the London Extradition Scheme, which provides for the rendition of fugitive offenders among members of the Commonwealth of Nations [9].

While formal mutual assistance can be requested of any country (even in the absence of diplomatic relations), it is usually easier when prior treaty arrangements are in place. Even under the best of circumstances, the machinery of formal mutual assistance turns slowly. Requests must be processed through a central office in both requesting and requested countries, and usually requires approval at a ministerial or other high official level.

Where is the crime?

The question of who will prosecute a case of transnational cybercrime raises issues of jurisdiction. Traditionally, jurisdiction is based on four principles: territoriality; nationality; effects; and matters of universal jurisdiction [1, note 33, 17, 21]. According to the territoriality principle, sovereign states can assert jurisdiction over behaviour occurring within their territorial borders. The vast majority of criminal laws do just that.

According to the nationality principle, states can assert jurisdiction over behaviour involving their citizens as perpetrators, regardless of where the alleged conduct occurred. Citizens of the United States, Australia, and many other places can be prosecuted in their home countries for having had sex with children anywhere in the world, even where such conduct may not constitute a criminal offence in those countries.[12]

Under the effects principle, countries may assert jurisdiction over behaviour that affects their national interests, regardless of where it may have originated. A person who, on foreign soil, engages in an act of terrorism against an Australian citizen, or who assists others in entering Australia illegally, is similarly liable to prosecution in Australia.

Under principles of universal jurisdiction, countries can establish mechanisms to prosecute a person for conduct, regardless of where it was committed, that is deemed to be

[12] [See *Crimes (Child Sex Tourism) Amendment Act 1994* (Cth) which inserted new offences into the Crimes Act 1914 (Cth)].

a crime against humanity—e.g. genocide or slavery. Numerous countries have prosecuted persons for alleged war crimes committed both far away and long ago, particularly during World War Two in Europe. The International Criminal Court now provides a forum for prosecution of such crimes.[13]

Box 6: Extraterritorial Jurisdiction

Australian law provides for jurisdiction over certain cybercrime offences where
(a) the conduct constituting the alleged offence occurs:
(i) wholly or partly in Australia; or
(ii) wholly or partly on board an Australian aircraft or an Australian ship; or

(b) the conduct constituting the alleged offence occurs wholly outside Australia and a result of the conduct occurs:
(i) wholly or partly in Australia; or
(ii) wholly or partly on board an Australian aircraft or an Australian ship; or

(c) the conduct constituting the alleged offence occurs wholly outside Australia and:
(i) at the time of the alleged offence, the person is an Australian citizen; or
(ii) at the time of the alleged offence, the person is a body corporate incorporated by or under a law of the Commonwealth or of a State or Territory;

Who will prosecute?

The decision on where a given crime will be prosecuted will depend on the laws, priorities, resources and capacities of the respective countries involved. In some cases, extradition will be precluded by law; some states will not extradite one of their own citizens; few if any will extradite a juvenile. In ordinary matters, authorities may be content to leave prosecution to the state from which the accused committed the alleged crime.

Box 7: Foreign Prosecution

A cybercrime committed from Country A to Country B, assuming a suspect has been identified and the behaviour in question violated the laws of both countries, raises the question of who will prosecute. Perhaps the easiest solution is to leave the matter to authorities in the country from which the perpetrator undertook the alleged criminal activity. It is a much less costly and time-consuming path to take than extradition. Perhaps the most publicized example of the host country prosecuting a cross national offender was the case of the 15 year old Canadian youth ("Mafia Boy") who launched distributed denial of service attacks against Yahoo, Amazon.com and other prominent e-commerce sites in February 2000. The extradition of a juvenile was precluded under Canadian law, and US authorities requested that the young accused be dealt with appropriately by their Canadian counterparts. In September 2001, "Mafia Boy" was sentenced to eight months in a youth detention centre.

[13] Criminal Code Act 1995 (Cth), as introduced by the Cybercrime Act 2001 (Cth) and augmented by subsequent legislation including the Crimes Legislation Amendment (Telecommunications Offences and Other Measures) Act (No. 2) 2004 (Cth), s476.3

The framework of treaties and other agreements which can form the basis for mutual assistance is far from perfect. Soma et al. [20], 326) refer to a patch-work atmosphere of varying extradition standards. Moreover, costs associated with mutual legal assistance are borne by the party providing assistance. This creates hardship where small countries, which may never request mutual assistance of their own motion, are required to process requests from more affluent countries. This may lead to the impression that poor countries may thus be bound by treaty to subsidizing the rich. However, often countries seeking legal assistance do cover the corresponding costs. In addition, cost relief and sharing provisions are contained in the UN Convention against Transnational Organized Crime, which may sometimes apply to cyber crimes.[14]

Box 8: Extradition

One of the more celebrated cases of the 1990s entailed an attack against Citibank by a young Russian. Using his own computer in Russia, the accused obtained unauthorized access to the bank's servers in the United States. He enlisted a number of confederates to open up bank accounts around the world, then instructed the Citibank computer to transfer funds to the various accounts. When the scheme was discovered and the accused identified as the perpetrator, an arrest warrant was issued in a United States Federal Court. There was no extradition treaty at the time between Russia and the United States, but the accused made the mistake of visiting England to attend a computer exhibition. British authorities were obliged to cooperate in extraditing him to face charges in the United States. Under the extradition arrangements in force between the United Kingdom and the United States, United Kingdom authorities could assist as long as the offence with which the accused was charged had some equivalent in United Kingdom law. The accused applied for a writ of habeas corpus challenging the extradition, arguing *inter alia*, that the appropriation had taken place in Russia, where his computer keyboard was located, not in the United States. The Court held that the accused's physical presence 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; had he been operating from the United Kingdom rather than Russia, English courts would have jurisdiction. The accused was eventually extradited to the United States, where he was convicted and sent to prison. (In re Levin [1997] 3 All ER 289)
http://www.parliament.the-stationery-office.co.uk/pa/ld199798/ldjudgmt/jd970619/levin.htm

Given that international cooperation, and especially mutual assistance, depends to a great extent on dual criminality, the goal of legal harmonization has taken on great importance. While perfect uniformity of substantive and procedural criminal law across the world's legal systems is not feasible, a degree of consistency on core offences is more or less achievable.

The United Nations has also played an important role in fostering international cooperation in response to cybercrime. In 1990, the Eighth United Nations Congress on the Prevention of Crime and the Treatment of Offenders passed a resolution calling on Member States to intensify their efforts to combat cyber crime, in particular by modernising their national laws. In 1994 it published the *UN Manual on the Prevention and Control of Computer-Related Crime*. It held workshops on cybercrime in conjunction with the 10th United Nations Crime Congress (Vienna 2000) and the 11th Congress (Bangkok 2005).

[14] When, for example, they are committed by an organized criminal group.

Another example of the move toward harmonization is the Council of Europe Convention on Cyber Crime, to date the most widespread and comprehensive initiative in international cooperation in cybercrime control. The convention seeks to achieve a degree of consistency in substantive criminal law, evidence and procedure, as well as expedited mutual assistance in cases of cyber crime committed across national frontiers. Even during its long drafting stage (over 4 years and producing 27 drafts), it provided guidance for non-European states involved in developing their own legislation. The Convention on Cybercrime was formally adopted by the Council of Europe in Budapest in November 2001. The Convention came into force in July 2004.[15]

The challenge of responding to cybercrime is compounded by the speed with which an offence can be committed, and the volatility of digital evidence. Immediate investigative response is often essential. Originally created in 1997 by the G8, a 24/7 network of contact points exists to provide informal assistance. By 2006, 45 countries had joined the network.

Despite the progress made to date in furtherance of international cooperation to combat cybercrime, a great deal more remains to be accomplished. There is a need for "fast freeze" preservation of digital evidence; consistency in procedural law that would permit real time tracing across multiple jurisdictions; expansion of the 24/7 contact system, and expedited (email) request for mutual legal assistance.

Challenges for the prosecutor

Framing the charge

In addition to the various matters raised above, one of the more important challenges facing any prosecutor is to get the charge right. Whether in terrestrial space or in cyber space, this means fitting the facts to the law. For example (in common law jurisdictions), in a homicide where evidence of premeditation is lacking, one does not normally charge a suspect with murder. Manslaughter (which does not require proof of intent to kill) is more appropriate.

Box 9: Inappropriate charges

A number of prosecutions have also foundered on what turned out to be the inappropriate charge of unauthorized access to a computer system. Simply picking the wrong section of an act can get a prosecutor into trouble. In an early UK case, the accused were officers in the Metropolitan Police who obtained car registration and ownership details from the Police National Computer. The data were for their personal use, not police business. They were charged with, and convicted of, unauthorized access under section 1 of the Computer Misuse Act. They successfully appealed the conviction on the grounds that their access to the police computer was authorized; it was the subsequent activity that exceeded the bounds of their authorization. The Court observed that the defendants could have been prosecuted under section 17(2) of the Data Protection Act 1984, which deals with improper use of data. Legislation embracing Art 2 of the Council of Europe Cyber Crime Convention, which prohibits unauthorized access to the whole or part of a computer system, would have covered this, as would 18 U.S. Code Section 1030, which includes 'exceeding authorized access' ([1988] 1 Cr. App. Rep. 1).

[15] http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm (visited 28 September 2007)

In some cases, prosecutors are able to fit pre-digital law to digital realities. Just as the law of theft was interpreted in some jurisdictions to include theft of intangible property (such as electricity) so too was the law of obscenity stretched slightly to embrace digital images.

Anticipating defence strategies

Depending upon the legal system in question, prosecutors may be called upon to rebut a variety of defense strategies. Some of these may be traditional, common to a range of ordinary terrestrial offences, while others may be unique to cybercrime. Defendants may challenge the validity of a search warrant, or may complain that investigators exceeded the scope of the warrant in the course of their search. They may argue that the evidence was contaminated in the course of seizure, or was somehow altered between the time of seizure and the time it was presented in court. In jurisdictions where conviction requires proof beyond reasonable doubt, prosecutors must be able to refute these contentions.

The defence may question the identity of the author of the evidence in question ('It wasn't me; it was somebody else'). In the digital age, some defendants might claim that their computer had been infected by a Trojan Horse virus, and that the incriminating evidence had been planted there by person or persons unknown. Others may argue that numerous people in the household had access to the computer in question and any one might have been responsible for the offence in question.

Managing large volumes of evidence

Among the challenges faced by today's investigators and prosecutors is the enormous increase in storage capacity of today's computers. This poses considerable challenges to effective and efficient searches. Pollitt (2003) reports that hard drive capacity increased by over 6000% during the 5 year period ending in 2002. A typical laptop can now hold hundreds of thousands of pages of data. Not only does this complicate the task of finding evidence that one knows exists, it greatly increases the challenge of looking for evidence that may exist. Moreover, prosecutors are required to distil and present the evidence in digestible form to judges and juries.

Drafting and executing search warrants in the digital age are particularly challenging tasks, as the material sought might be commingled with vast amounts of other data, irrelevant to the matter under investigation. Moreover, the medium in which they are stored might be integral to the operational information system of an otherwise legitimate enterprise. Unless the system itself was an instrument of the alleged offence, seizure of the entire system might cause undue loss to proprietors or to innocent clients. A classic illustration of this was the case, *Steve Jackson Games, Inc. v United States Secret Service* (1994) 36 F.3d 457 (5th Cir), in which the United States Secret Service seized hardware and data files from a small Texas games manufacturer and Internet service provider, nearly putting it out of business. Neither the company nor its principal was ever prosecuted; the material seized was thought to contain evidence of an offence by one of the company's customers.

Prosecuting juveniles

The growth and diffusion of information technology provides juveniles with the capacity to do harmful acts that were simply unachievable before the digital age. The enormous growth

in computing power and accessibility, and the relative technological sophistication of young people today, have given rise to some dramatic cases. Juveniles have succeeded in penetrating the computer systems of sensitive defence installations; shutting down air traffic control systems; clogging servers of large e-commerce sites; and manipulating shares traded on stock exchanges.

It is a basic principle of juvenile justice that young people should face criminal proceedings only as a last resort. Authorities in many criminal justice systems avoid bringing the full force of the law against young offenders. Elaborate systems of counseling and diversion have been created to keep young offenders out of court. Nevertheless, authorities in some countries will pursue juvenile computer criminals in highly visible cases. Although the offenders in question are unlikely to receive heavy sentences, there is a perceived need to proceed with prosecution in some cases in order to achieve general deterrence and to publicise the fact that the conduct in question is unacceptable and illegal.

Technical legal assistance and capacity building

Countries that are developing legislation to combat cybercrime need not work in isolation. Countries on the leading edge of digital technology have years of experience that most are happy to share. Existing law and policy of many individual nations is readily accessible.[16] So too is the collective experience of groups of nations such as the Council of Europe or the G8. Various models of legislation are available for adoption by nations entering the digital age, or for adaptation in a manner consistent with their respective legal cultures and constitutional frameworks.

Digital technology continues to evolve, and with the increased prevalence of computing, the criminal exploitation of this technology can only become more prevalent and more sophisticated. Because the global nature of cyber crime means that attacks may originate almost anywhere, criminal justice officials of all nations, regardless of their location vis-à-vis the digital divide, are well advised to keep abreast of legal, technological, economic and social developments relating to computer crime and its control.

Capacity building must therefore take place within and between nations. In the more technologically sophisticated jurisdictions, steps are being taken to ensure a degree of prosecutorial familiarity with digital technology. In Korea, the Supreme Public Prosecutor's Office established the 'Computer Crime Investigation Division' under the direction of its Central Investigation Department in February 2000 [16]. In the United States, U.S. Attorneys' offices in every federal judicial district have at least one assistant designated as the Computer and Telecommunications Coordinator. Each has received specialized training in computer crime and is primarily responsible for providing technical expertise within their district (United States Department of Justice 2001, 5).

The Commonwealth Secretariat provides technical legal support to members particularly in support of mutual legal assistance arrangements and alerts member states to developments in technology law [6]. The Bangkok Declaration reaffirmed the fundamental importance of implementing existing instruments and the further development of national measures and international cooperation in criminal matters, such as consideration of strengthening and augmenting measures against cybercrime. It also noted that globalization

[16] http://www.austlii.edu.au/au/legis/cth/consol_act/ca2001112/. http://www.usdoj.gov/criminal/cybercrime/17_18red.htm

and new technologies have been accompanied by the abuse of those technologies for criminal purposes. It went on to welcome efforts to enhance and supplement existing cooperation to prevent, investigate and prosecute high-technology and computer-related crime, including by developing partnerships with the private sector. Finally, it recognized the important contribution of the United Nations to regional and other international forums in the fight against cybercrime and invited the Commission on Crime Prevention and Criminal Justice to examine the feasibility of providing further assistance in that area under the aegis of the United Nations in partnership with other similarly focused organizations[17].

The role of the private sector in cyber crime control

Effective and efficient control of cyber crime requires more that cooperation among law enforcement agencies, however. The role of the communications and information technology industries in designing products that are resistant to crime and that facilitate detection and investigation, cannot be understated. And the actual collaboration of private sector organizations with public law enforcement agencies is already becoming a fact of life in some countries. Pacific Century Cyberworks (PCCW) (with 680,000 subscribers, Hong Kong's largest Internet Service Provider) has a department dedicated to assisting Hong Kong Police (HKP). HKP conduct joint investigations with PCCW staff.

Conclusion

Prosecutors play a pivotal role in the criminal justice system. In many countries, they are the drivers of reform and the guardians of justice. The major challenges that cyber crime poses for nations on both sides of the digital divide are challenges for prosecutors. In many places, it will be the responsibility of prosecutors to ensure that their criminal justice systems are equipped to guarantee security and prosperity in cyberspace and to safeguard human rights.

Ideal policy directions have been nicely mapped out by Bullwinkel [4] These include

- the enactment of substantive and procedural laws adequate to cope with current and anticipated manifestations of cyber crime;
- the development of forensic computing skills by law enforcement and investigative personnel, and judicial officers;
- the achievement of a modicum of legal harmonization, ideally at a global level;
- the creation of mechanisms for operational cooperation between law enforcement agencies from different countries—24/7 points of contact for investigators, and mechanisms for mutual assistance in cyber criminal matters generally.

Many basic features of cyber crime, like "old wine in new bottles" are already familiar to prosecutors. Where the computer is the instrument of a crime, the substantive criminal law may already be in place, and may easily accommodate the facts of the case. But there are those aspects of cyber crime that pose special problems. As we have seen, digital technology facilitates transnational offending. Cross-border criminality is by no means unique to the digital age, but it has become more common. Today, even children can do it. The challenges of cross-national cyber crime are compounded by the so-called "digital

[17] See Bangkok Declaration 2005, Synergies and Responses: Strategic Alliances in Crime Prevention and Criminal Justice; available at http://www.unodc.org/pdf/crime/congress11/BangkokDeclaration.pdf

divide" which reflects the limited capacity of some countries to respond to cyber crime. This reinforces the importance to all nations of capacity building, especially in those nations that have just begun to enter the digital age.

Whether the crime is a new one, like phishing [12], or a more conventional fraud committed with new technology, the intangible nature of digital evidence is also a challenge for prosecutors. Assembling evidence, preserving its integrity, and presenting it in a comprehensible manner to a court has always been the prosecutor's role. But judges and juries who are unfamiliar with high technology may be uncomfortable with evidence in digital form. And skilled defence counsel may seek to sow the seeds of doubt by suggesting that computer malfunction or human intervention contaminated the evidence in question. The accused, moreover, may argue that it was not he or she who committed the criminal act, but rather someone else with either direct or remote access to the computer. One recognizes that capacity building is important in advanced industrial nations, as well as those on the other side of the digital divide.

As we have seen, technology evolves faster than law. This is particularly challenging when it comes to new crimes, such as the dissemination of worms and viruses, and distributed denial of service attacks. Cyber criminals have gone free because the substantive criminal law had yet to be brought into the digital age. But out of date or inflexible laws may also impede the prosecution of conventional crimes committed with new technologies. The law of fraud should be sufficiently adaptable to prohibit deception of a computer no less than deception of a human being.

Another significant challenge is posed by the reluctance of many victims of cyber crime to report in the first place. Commercial institutions in particular may be reluctant to disclose their vulnerability, or their security breaches, to clients and shareholders; individual victims may feel that the police are unwilling or unable to assist.

To sum up, it is useful to note once again that crime follows opportunity. Continuing developments in digital technology, and its diffusion around the world, will provide new opportunities for criminal exploitation. It is incumbent upon prosecutors to work towards the control of cyber crime, while allowing the fullest use of digital technology for legitimate purposes. One can build upon Santayana's dictum that those who forget the past are condemned to repeat it. Today, those who fail to anticipate the future are in for a rude shock when it arrives.

References

1. Bellia, P. L. (2001). Chasing bits across borders. *University of Chicago Legal Forum*, 35–101.
2. Brenner, S., & Frederiksen B. (2001). Computer searches and seizures: Some unresolved issues. *Michigan Telecommunications and Technology Law Review, 8*, 39–114.
3. Brenner, S., & Schwerha, J. J. (2002). Transnational evidence gathering and local prosecution of cybercrime. *John Marshall Journal of Computer and Information Law, 20*, 347.
4. 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: Hong Kong University Press.
5. Coll, S., & Glasser, S. (2005). In London, islamic radicals found a haven. *The Washington Post*, July 10, A01. Retrieved July 26, 2005, from http://www.washingtonpost.com/wp-dyn/content/article/2005/07/09/AR2005070901390_pf.html.
6. Commonwealth Secretariat (2004). *LAWDevelopment*: Issues of the Commonwealth Issue 4. http://www.thecommonwealth.org/law.
7. Denning, D. (2000). *Cyberterrorism*. Testimony before the special oversight panel on terrorism, committee on armed services, U.S. House of Representatives, May 23, 2000. Retrieved March 12, 2005, from http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html.

8. Drozdova, E. (2001). Civil liberties and security in cyberspace. In A. Sofaer & S. Goodman (Eds.), *The transnational dimension of cyber crime and terrorism* (pp. 183–220). Stanford: Hoover Institution Press. http://www.hoover.org/publications/books/cybercrime.html.
9. Grabosky, P. (2004). The global dimension of cybercrime. *Global Crime, 6*(1), 146–157.
10. Grabosky, P., Smith, R., & Dempsey, G. (2001). *Electronic theft: Unlawful acquisition in cyberspace*. Cambridge: Cambridge University Press.
11. Johnson, D. (2002). *The Japanese way of justice: Prosecuting crime in Japan*. New York: Oxford University Press.
12. Krone, T. (2005). *Phishing. High Tech Crime Brief No 9*. Canberra: Australian Institute of Criminology. Retrieved July 5, 2005, from http://www.aic.gov.au/publications/htcb/htcb009.html.
13. McKemmish, R. (1999). *What is forensic computing? Trends and issues in crime and criminal justice #118*. Canberra: Australian Institute of Criminology. http://www.aic.gov.au/publications/tandi/ti118.pdf.
14. Morris, S. (2004a). *The future of netcrime now: Part 1—threats and challenges home office online report 62/04*. Retrieved March 12, 2005, from http://www.homeoffice.gov.uk/rds/pdfs04/rdsolr6204.pdf.
15. Nasheri, H. (2005). *Economic espionage and industrial spying*. Cambridge: Cambridge University Press.
16. Park, E. (2001). *Analysis of Internet crime in Korea and countermeasures*. Paper presented to the Sixth Annual Conference of the International Association of Prosecutors, Sydney, Australia, September 2–7, 2001. http://www.iap.nl.com/speeches2/internetcrime.html.
17. Podgor, E. (2002). International computer fraud: A paradigm for limiting national jurisdiction. *UC Davis Law Review, 35*, 267–317.
18. Pollitt, M. (2003). "Digital evidence in internet time". In R. Broadhurst (Ed.), *Bridging the GAP: A Global Alliance on Transnational Organised Crime*. Hong Kong: Hong Kong Police.
19. Smith, R. G., Grabosky, P., & Urbas, G. (2004). *Cyber criminals on trial*. Cambridge: University Press Cambridge.
20. Soma, J. T., Muther, T. F. Jr., & Brisette, H. (1997). Transnational extradition for computer crimes: Are new treaties and laws needed? *Harvard Journal on Legislation, 34*, 317–370.
21. Tan, K. H. (2000). *Prosecuting foreign based computer crime: International law and technology collide*. Presented at the Symposium on the Rule of Law in the Global Village, Palermo, Italy, December 12–14, 2000. http://www.undcp.org/adhoc/palermo/convmain.html.
22. Thomas, T. L (2003). Al Qaeda and the Internet: The danger of "cyberplanning". *Parameters, 33*(1), 112–123. Retrieved March 12, 2005, from http://carlisle-www.army.mil/usawc/Parameters/03spring/thomas.htm.
23. UNAFEI (1995). *Criminal justice profiles of Asia*. Tokyo: United Nations Asia and Far East Institute for the Prevention of Crime and the Treatment of Offenders.
24. United States Department of Justice (2002). *Searching and seizing computers and obtaining electronic evidence in criminal investigations*. Washington, DC: US Department of Justice. Retrieved July 6, 2005, from http://www.cybercrime.gov/s&smanual2002.htm.