CYBER CRIME AND INFORMATION WARFARE

Dr Peter Grabosky
Australian Institute of Criminology, ACT

Paper presented at the Transnational Crime Conference
convened by the Australian Institute of Criminology
in association with the Australian Federal Police and
Australian Customs Service
and held in Canberra, 9-10 March 2000

Introduction

Willie Sutton, a notorious American bank robber of a half century ago, was once asked why he persisted in robbing banks. "Because that's where the money is," he is said to have replied.[1] The theory that crime follows opportunity has become established wisdom in criminology; opportunity reduction has become one of the fundamental principles of crime prevention.

But there is more to crime than opportunity. Crime requires a pool of motivated offenders, and a lack of what criminologists would refer to as "capable guardianship"; someone to mind the store, so to speak.

These basic principles of criminology apply to computer related crime no less than they do to bank robbery or to shop lifting. They will appear from time to time throughout the following discussion. Not all of these factors are amenable to control by governments alone. It follows, therefore, that a variety of institutions will be required to control computer related crime.

This paper discusses current and emerging forms of computer-related illegality. It reviews nine generic forms of illegality involving information systems as instruments or as targets of crime.

It will also discuss issues arising from the global reach of information systems. It is trite to describe the ways in which computers have, figuratively speaking, made the world a smaller place. The corresponding potential for trans-jurisdictional offending will pose formidable challenges to law enforcement. For some crimes, this will necessitate a search for alternative solutions.

The following pages will suggest that much computer-related illegality lies beyond the capacity of contemporary law enforcement and regulatory agencies alone to control, and that security in cyberspace will depend on the efforts of a wide range of institutions, as well as on a degree of self-help by potential victims of cyber-crime.

The ideal configuration may be expected to differ, depending upon the activity in question, but is likely to entail a mix of law enforcement, technological and market solutions. The paper will conclude with a discussion of the most suitable institutional configuration to address those forms of computer-related crime which have been identified.

Before we begin to review the various forms of criminality involving information systems as instruments and/or as targets, and the most appropriate means of controlling them, let us first look at the questions of motivation and of opportunity.

Motivations of Computer Criminals

The motivations of those who would commit computer related crime are diverse, but hardly new. Computer criminals are driven by time-honoured motivations, the most obvious of which are greed, lust, power, revenge, adventure, and the desire to taste "forbidden fruit". The ability to make an impact on large systems may, as an act of power, be gratifying in and of itself. The desire to inflict loss or damage on another may also spring from revenge, as when a disgruntled employee shuts down an employer's computer system, or to ideology, as when one defaces the

[1] There remains considerable doubt whether the words were Sutton's, or rather those of an imaginative journalist. See Ralph Keyes, Nice Guys Finish Seventh:False Phrases, Spurious Sayings and Familiar Misquotations. Harper Collins New York:1993, p 16.

web page of an institution that one regards as abhorrent. Much activity on the electronic frontier entails an element of adventure, the exploration of the unknown. The very fact that some activities in cyberspace are likely to elicit official condemnation is sufficient to attract the defiant, the rebellious, or the irresistibly curious. Given the degree of technical competence required to commit many computer-related crimes, there is one other motivational dimension worth noting here. This, of course, is the intellectual challenge of mastering complex systems.

None of the above motivations is new. The element of novelty resides in the unprecedented capacity of technology to facilitate acting on these motivations.

Increasing Opportunities for Computer-Related Crime

Recent and anticipated changes in technology arising from the convergence of communications and computing are truly breathtaking, and have already had a significant impact on many aspects of life. Banking, stock exchanges, air traffic control, telephones, electric power, and a wide range of institutions of health, welfare, and education are largely dependent on information technology and telecommunications for their operation. We are moving rapidly to the point where it is possible to assert that "everything depends on software" (Edwards 1995). The exponential growth of this technology, the increase in its capacity and accessibility, and the decrease in its cost, has brought about revolutionary changes in commerce, communications, entertainment, and also crime. Along with this greater capacity, however, comes greater vulnerability. Information technology has begun to provide criminal opportunities of which Willie Sutton would never have dreamed.

Statistics on computer use and connectivity are notoriously evanescent. They are out of date before they appear in print. Suffice it to say that the number of people with internet connections will continue to increase dramatically, as will the volume of electronic commerce in Australia, and around the world.

Not only does the increasing connectivity increase the number of prospective victims of computer related crime, it also increases the number of prospective offenders.

Varieties of Computer-Related Crime

The variety of criminal activity which can be committed with or against information systems is surprisingly diverse. Some of these are not really new in substance; only the medium is new. Others represent new forms of illegality altogether.

The following generic forms of illegality involve information systems as instruments and/or as targets of crime. These are not mutually exclusive, nor is the following list necessarily exhaustive.

A. Theft of Information Services

The "phone phreakers" of three decades ago set a precedent for what has become a major criminal industry. By gaining access to an organisation's telephone switchboard (PBX) individuals or criminal organisations can obtain access to dial-in/dial-out circuits and then make their own calls or sell call time to third parties (Gold 1999). Offenders may gain access to the switchboard by impersonating a technician, by fraudulently obtaining an employee's access code, or by using software available on the internet. Some sophisticated offenders loop between PBX systems to evade detection. Additional forms of service theft include capturing "calling card" details and on-selling calls charged to the calling card account, and counterfeiting or illicit reprogramming of stored value telephone cards.

It has been suggested that as long ago as 1990, security failures at one major telecommunications carrier cost approximately £290 million, and that more recently, up to 5% of total industry turnover has been lost to fraud (Schieck 1995: 2-5; Newman 1998). Costs to individual subscribers can also be significant In one case, computer hackers in the United States illegally obtained access to Scotland Yard's telephone network and made £620,000 worth of international calls for which Scotland Yard was responsible (Tendler and Nuttall 1996).

B. Communications in Furtherance of Criminal Conspiracies

Just as legitimate organisations in the private and public sectors rely upon information systems for communications and record keeping, so too are the activities of criminal organisations enhanced by technology.

There is evidence of telecommunications equipment being used to facilitate organised drug trafficking, gambling, prostitution, money laundering, child pornography and trade in weapons (in those jurisdictions where such activities are illegal). The use of encryption technology may place criminal communications beyond the reach of law enforcement.

The use of computer networks to produce and distribute child pornography has become the subject of increasing attention. Today, these materials can be imported across national borders at the speed of light (Grant, David and Grabosky 1997). The more overt manifestations of internet child pornography entail a modest degree of organisation, as required by the infrastructure of IRC and WWW, but the activity appears largely confined to individuals.

By contrast, some of the less publicly visible traffic in child pornography activity appears to entail a greater degree of organisation. Although knowledge is confined to that conduct which has been the target of successful police investigation, there appear to have been a number of networks which extend cross-nationally, use sophisticated technologies of concealment, and entail a significant degree of coordination.

Illustrative of such activity was the Wonderland Club, an international network with members in at least 14 nations ranging from Europe, to North America, to Australia. Access to the group was password protected, and content was encrypted. Police investigation of the activity, codenamed "Operation Cathedral" resulted in approximately 100 arrests around the world, and the seizure of over 100,000 images in September, 1998.

C. Telecommunications Piracy

Digital technology permits perfect reproduction and easy dissemination of print, graphics, sound, and multimedia combinations. The temptation to reproduce copyrighted material for personal use, for sale at a lower price, or indeed, for free distribution, has proven irresistible to many.

This has caused considerable concern to owners of copyrighted material. Each year, it has been estimated that losses of between US$15 and US$17 billion are sustained by industry by reason of copyright infringement (United States, Information Infrastructure Task Force 1995, 131).

The Software Publishers Association has estimated that $7.4 billion worth of software was lost to piracy in 1993 with $2 billion of that being stolen from the Internet (Meyer and Underwood 1994).

Ryan (1998) puts the cost of foreign piracy to American industry at more than $10 billion in 1996, including $1.8 billion in the film industry, $1.2 billion in music, $3.8 billion in business application software, and $690 million in book publishing.

According to the Straits Times (8/11/99) A copy of the most recent James Bond Film *The World is Not Enough*, was available free on the internet before its official release.

When creators of a work, in whatever medium, are unable to profit from their creations, there can be a chilling effect on creative effort generally, in addition to financial loss.

D. Dissemination of Offensive Materials

Content considered by some to be objectionable exists in abundance in cyberspace. This includes, among much else, sexually explicit materials, racist propaganda, and instructions for the fabrication of incendiary and explosive devices. Telecommunications systems can also be used for harassing, threatening or intrusive communications, from the traditional obscene telephone call to its contemporary manifestation in "cyber-stalking", in which persistent messages are sent to an unwilling recipient.

One man allegedly stole nude photographs of his former girlfriend and her new boyfriend and posted them on the Internet, along with her name, address and telephone number. The unfortunate couple, residents of Kenosha, Wisconsin, received phone calls and e-mails from strangers as far away as Denmark who said they had seen the photos on the Internet. Investigations also revealed that the suspect was maintaining records about the woman's movements and compiling information about her family (Spice and Sink 1999).

In another case a rejected suitor posted invitations on the Internet under the name of a 28-year-old woman, the would-be object of his affections, that said that she had fantasies of rape and gang rape. He then communicated via email with men who replied to the solicitations and gave out personal information about the woman, including her address, phone number, details of her physical appearance and how to bypass her home security system. Strange men turned up at her home on six different occasions and she received many obscene phone calls. While the woman was not physically assaulted, she would not answer the phone, was afraid to leave her home, and lost her job (Miller 1999; Miller and Maharaj 1999).

One former university student in California used email to harass 5 female students in 1998. He bought information on the Internet about the women using a professor's credit card and then sent 100 messages including death threats, graphic sexual descriptions and references to their daily activities. He apparently made the threats in response to perceived teasing about his appearance (Associated Press 1999a).

Computer networks may also be used in furtherance of extortion. The Sunday Times (London) reported in 1996 that over 40 financial institutions in Britain and the United States had been attacked electronically over the previous three years. In England, financial institutions were reported to have paid significant amounts to sophisticated computer criminals who threatened to wipe out computer systems. (The Sunday Times, June 2, 1996). The article cited four incidents between 1993 and 1995 in which a total of 42.5 million Pounds Sterling were paid by senior executives of the organisations concerned, who were convinced of the extortionists' capacity to crash their computer systems (Denning 1999 233-4).

One case, which illustrates the transnational reach of extortionists, involved a number of German hackers who compromised the system of an Internet service provider in South Florida, disabling eight of the ISPs ten servers. The offenders obtained personal information and credit card details of 10,000 subscribers, and, communicating via electronic mail through one of the compromised accounts, demanded that US$30,000 be delivered to a mail drop in Germany. Co-operation between US and German authorities resulted in the arrest of the extortionists (Bauer 1998).

More recently, an extortionist in Eastern Europe obtained the credit card details of customers of a North American based on-line music retailer, and published some on the Internet when the retailer refused to comply with his demands (Markoff 2000).

E. Electronic Money Laundering and Tax Evasion

For some time now, electronic funds transfers have assisted in concealing and in moving the proceeds of crime. Emerging technologies will greatly assist in concealing the origin of ill-gotten gains. Legitimately derived income may also be more easily concealed from taxation authorities. Large financial institutions will no longer be the only ones with the ability to achieve electronic funds transfers transiting numerous jurisdictions at the speed of light. The development of informal banking institutions and parallel banking systems may permit central bank supervision to be bypassed, but can also facilitate the evasion of cash transaction reporting requirements in those nations which have them. Traditional underground banks, which have flourished in Asian countries for centuries, will enjoy even greater capacity through the use of telecommunications.

With the emergence and proliferation of various technologies of electronic commerce, one can easily envisage how traditional countermeasures against money laundering and tax evasion may soon be of limited value. I may soon be able to sell you a quantity of heroin, in return for an untraceable transfer of stored value to my “smart-card”, which I then download anonymously to my account in a financial institution situated in an overseas jurisdiction which protects the privacy of banking clients. I can discreetly draw upon these funds as and when I may require, downloading them back to my stored value card (Wahlert 1996).

F. Electronic Vandalism and Terrorism

As never before, western industrial society is dependent upon complex data processing and telecommunications systems. Damage to, or interference with, any of these systems can lead to catastrophic consequences. Whether motivated by curiosity or vindictiveness electronic intruders cause inconvenience at best, and have the potential for inflicting massive harm (Hundley and Anderson 1995, Schwartau 1994).

While this potential has yet to be realised, a number of individuals and protest groups have hacked the official web pages of various governmental and commercial organisations (Rathmell 1997). http://www.2600.com/hacked_pages/ (visited 4 January 2000). This may also operate in reverse: early in 1999 an organised hacking incident was apparently directed at a server which hosted the Internet domain for East Timor, which at the time was seeking its independence from Indonesia (Creed 1999).

Defence planners around the world are investing substantially in information warfare - means of disrupting the information technology infrastructure of defence systems (Stix 1995).[2] Attempts were made to disrupt the computer systems of the Sri Lankan Government (Associated Press 1998), and of the North Atlantic Treaty Organization during the 1999 bombing of Belgrade (BBC 1999).

G. Sales and Investment Fraud

As electronic commerce becomes more prevalent, the application of digital technology to fraudulent endeavours will be that much greater. The use of the telephone for fraudulent sales pitches, deceptive charitable solicitations, or bogus investment overtures is increasingly common. Cyberspace now abounds with a wide variety of investment opportunities, from traditional securities such as stocks and bonds, to more exotic opportunities such as coconut farming, the sale and leaseback of automatic teller machines, and worldwide telephone lotteries (Cella and Stark 1997 837-844). Indeed, the digital age has been accompanied by unprecedented opportunities for misinformation. Fraudsters now enjoy direct access to millions of prospective victims around the world, instantaneously and at minimal cost.

Classic pyramid schemes and "Exciting, Low-Risk Investment Opportunities" are not uncommon. The technology of the World Wide Web is ideally suited to investment solicitations. In the words of two SEC staff “At very little cost, and from the privacy of a basement office or living room, the fraudster can produce a home page that looks better and more sophisticated than that of a Fortune 500 company” (Cella and Stark 1997, 822).

H. Illegal Interception of Telecommunications

Developments in telecommunications provide new opportunities for electronic eavesdropping. From activities as time-honoured as surveillance of an unfaithful spouse, to the newest forms of political and industrial espionage, telecommunications interception has increasing applications. Here again, technological developments create new vulnerabilities. The electromagnetic signals emitted by a computer may themselves be intercepted. Cables may act as broadcast antennas. Existing law does not prevent the remote monitoring of computer radiation.

It has been reported that the notorious American hacker Kevin Poulsen was able to gain access to law enforcement and national security wiretap data prior to his arrest in 1991 (Littman 1997). In 1995, hackers employed by a criminal organisation attacked the communications system of the Amsterdam Police. The hackers succeeded in gaining police operational intelligence, and in disrupting police communications (Rathmell 1997).

I. Electronic Funds Transfer Fraud

Electronic funds transfer systems have begun to proliferate, and so has the risk that such transactions may be intercepted and diverted. Valid credit card numbers can be intercepted electronically, as well as physically; the digital information stored on a card can be counterfeited.

[2] See also the website of the Institute for the Advanced Study of Information Warfare (IASIW) http://www.psycom.net/iwar.1.html

Of course, we don't need Willie Sutton to remind us that banks are where they keep the money. In 1994, a Russian hacker Vladimir Levin, operating from St Petersburg, accessed the computers of Citibank's central wire transfer department, and transferred funds from large corporate accounts to other accounts which had been opened by his accomplices in The United States, the Netherlands, Finland, Germany, and Israel. Officials from one of the corporate victims, located in Argentina, notified the bank, and the suspect accounts, located in San Francisco, were frozen. The accomplice was arrested. Another accomplice was caught attempting to withdraw funds from an account in Rotterdam. Although Russian law precluded Levin's extradition, he was arrested during a visit to the United States and subsequently imprisoned. (Denning 1999, 55.)

The above forms of computer-related crime are not necessarily mutually exclusive, and need not occur in isolation. Just as an armed robber might steal an automobile to facilitate a quick getaway, so too can one steal telecommunications services and use them for purposes of vandalism, fraud, or in furtherance of a criminal conspiracy.[3] Computer-related crime may be compound in nature, combining two or more of the generic forms outlined above.

A number of themes run through each of the forms of illegality described above. Foremost of these are the technologies for concealing the content of communications. Technologies of encryption can limit access by law enforcement agents to communications carried out in furtherance of a conspiracy, or to the dissemination of objectionable materials between consenting parties (Denning 1999).

Also important are technologies for concealing a communicator's identity. Electronic impersonation, colloquially termed "spoofing," can be used in furtherance of a variety of criminal activities, including fraud, criminal conspiracy, harassment, and vandalism. Technologies of anonymity further complicate the task of identifying a suspect (Froomkin 1995).

Beyond the aforementioned reluctance of victims to report, the technologies of secrecy and anonymity noted above often make detection of the offender extremely difficult. Those who seek to mask their identity on computer networks are often able to do so, by means of "looping", or "weaving" through multiple sites in a variety of nations. Anonymous remailers and encryption devices can shield one from the scrutiny of all but the most determined and technologically sophisticated regulatory and enforcement agencies. Some crimes do not result in detection or loss until some time after the event. Considerable time may elapse before the activation of a computer virus, or between the insertion of a "logic bomb" and its detonation.

The Size of the Problem

Estimating the incidence, prevalence, cost, or some other measure of computer related crime is a difficult challenge, Unlike bank robberies or fatal motor vehicle accidents, computer related crimes tend to defy quantification. Some of the most deftly perpetrated offences with or against information systems are never detected, not even by their victims; of those which are, some are concealed from authorities because disclosure could prove embarrassing or commercially inconvenient to victims.

Quantification can also be deceptive. What appears to be a trivial matter may in fact be the tip of a very big iceberg indeed. A classic illustration was provided by Stoll (1991) whose pursuit of a $.75 accounting error in a computer account led to an international espionage ring.

[3] The various activities of Kevin Mitnick, as described in Hafner and Markoff (1991) are illustrative.

Even qualitative descriptions can be illusory. Many people, regardless of their calling, are inclined to accentuate the problem, including boastful hackers, moral entrepreneurs, victims or commercial entities with a vested interest, not to mention the news media.

The Challenge of Controlling Computer-Related Crime

Motives

Recall from the earlier discussion that crime can be explained in part by the supply of motivated offenders. Given the diversity of computer related crime, it is not surprising that the various types of behaviour discussed above flow from a wide range of motives. Some of these are as old as human society, including greed, lust, revenge and curiosity. Revenge in the modern era can also entail an ideological dimension. Of considerable significance, if not unique to computer related crime, is the intellectual challenge of defeating a complex system. Motivations, whether on the part of individuals or in the aggregate, are very difficult to change. For this reason, the most strategically advantageous approaches to computer related crime will be concerned with the reduction of opportunities, and with the enhancement of guardianship.

Opportunities

While motives tend not to change, the variety and number of opportunities for cyber crime are proliferating. The exponential growth in connectivity of computing and communications creates parallel opportunities for prospective offenders, and parallel risks for prospective victims. As the internet becomes increasingly a medium of commerce, it will become increasingly a medium of fraud.

The most effective way of eliminating opportunities for on-line crime is simply to pull the plug. This is of course unrealistic; the affluent nations of the world are now highly dependent on information technology. For the poorer nations, information technology is probably a necessary, if not sufficient, path to economic development. Thus, the challenge lies in managing risk so as to achieve the maximum benefits which flow from new technologies, while minimising the downside. A merchant could scrutinise every credit card transaction to as to drastically reduce the risk of fraud, but in the process drive away legitimate customers. At a higher level, nations around the world are in the process of forging policies on where to draw the line on such fundamental questions as the balance between the citizen's privacy and the imperatives of law enforcement, and freedom of expression versus the protection of certain cultural values.

There are many technologies which reduce the opportunity to commit computer-related crime. Given that so much computer-related crime depends upon unauthorised access to information systems, access control and authentication technologies have become essential. Sophisticated advice and products for computer crime prevention are provided by one of the world's growth industries of today, namely computer security.

Denning (1999) offers a comprehensive inventory of technologies for reducing opportunities for computer crime. She describes technologies of encryption and anonymity, which permit concealment of the content of communications (such as a consumer's credit card details, or of the identity of the communicator (not all participants in discussion groups on reproductive health wish to disclose their identities). Denning also outlines technologies of authentication, from basic passwords, to various biometric devices such as finger print or voice recognition technology, and retinal imaging, which greatly enhance the difficulty of obtaining unauthorised access to information systems.

Virus detectors can identify and block malicious computer code; blocking and filtering programs can screen out unwanted content. A rich variety of commercial software now exists with which to block access to certain sites (Venditto 1996).

Guardians

The third basic factor which explains computer related crime is the absence of a capable guardian. Capable guardianship has evolved over human history, from feudalism, to the rise of the state and the proliferation of public institutions of social control, to the post-modern era in which employees of private security services vastly outnumber sworn police officers in many industrial democracies. Here again, it may be instructive to compare computer related crime with more conventional types of crime.

Guardianship against conventional crime involves preventive efforts on the part of prospective victims, contributions by members of the general public or commercial third parties, as well as the activities of law enforcement agencies. Indeed, it is often only when private efforts at crime prevention fail that the criminal process is mobilised. So it is that owners of motor vehicles are encouraged to lock their vehicles at all times, that insurance contracts may offer premium discounts for crime prevention measures such as theft alarms, and that some car parks have video surveillance or private security guards in attendance. Often, it is only when these systems fail that the assistance of law enforcement is sought.

Technology can also enhance guardianship. Denning (1999) describes various technologies for detecting attempted intrusions of information systems. Alarms can indicate when repeated login attempts fail because of incorrect passwords, or when access is sought outside of normal working hours. Other anomaly detection devices will identify unusual patterns of system use, including atypical destination and duration of telephone calls, or unusual spending patterns using credit cards.

Guardianship can also be enhanced by market forces. A market is currently emerging for internet service providers specialising in content suitable for family consumption, guaranteed to be free of sex, violence, and vilification. Market forces may also generate second-order controlling influences. As large organizations begin to appreciate their vulnerability to electronic theft or vandalism, they may be expected to insure against potential losses. It is very much in the interests of insurance companies to require appropriate security precautions on the part of their policyholders. Indeed, decisions to set and to price insurance may well depend upon security practices of prospective policy holders. Subcontractors may also be required to have strict IT integrity programs in place as a condition of doing business.

Citizen concern about the availability of undesirable content has given rise to the private monitoring and surveillance of cyberspace. Among the more prominent organizations involved in such surveillance are the Simon Wiesenthal Center, whose CyberWatch Hotline (http://www.wiesenthal.com/watch/whotline.htm) which invites notification of anti-Semitic and racist material.

Citizen co-production can complement activities undertaken by agencies of the state. An example of collaborative public-private effort in furtherance of controlling objectionable content is the Netherlands Hotline for Child Pornography on Internet, an initiative of the Foundation for Dutch Internetproviders (NLIP), the Dutch National Criminal Intelligence Service (CRI), Internet users, and the National Bureau against Racism (LBR). Users who encounter child pornography

originating in the Netherlands, identifiable by a domain name address ending in "nl" are encouraged to report the site to meldpunt@xs4all.nl. The originator is warned about the posting, and asked to desist from further such activity. If the warning is ignored, then the hotline will forward any available information to the vice-squad of the local police. [4]

The policing of terrestrial space is now very much a pluralistic endeavour, and so too is the policing of cyberspace. Responsibilities for the control of computer crime will be similarly shared between agents of the state, information security specialists in the private sector, and the individual user. In cyberspace today, as on terrestrial space two millennia ago, the first line of defence will be self defence - in other words, minding one's own store.

A. Investigative Issues

There will nevertheless be some matters which will require police attention, and these will lead us along some interesting paths. Whether the law can keep abreast of changing technologies (and the criminal exploitation of those technologies) has become an important question in the digital age.

Let me raise just a few rhetorical questions about the law relating to search and seizure of electronic evidence. These were formulated in October 1998 at a special expert working group meeting convened in Tokyo under the auspices of the United Nations. A full summary of the working group report, published by the United Nations in Vienna, is available on the World Wide Web at http://www.justinfo.net/UPLOAD/docs/report.htm .

(i) Does the law distinguish between the search and seizure of stored data in a computer, and the interception of data that is being communicated from one computer to another or within a computer system?

(ii) Can a person voluntarily provide law enforcement agents with electronic data that may afford evidence of a crime? Can a person voluntarily permit law enforcement agents to undertake a search for such data, rather than provide it to them? Could continuing cooperation of this nature by a person with law enforcement have a legal effect on the ability of law enforcement to obtain or use the data?

(iii) In most jurisdictions, the ability of law enforcement to obtain data that may afford evidence usually requires some form of prior judicial approval. What legal authority is required for obtaining electronic stored data without the consent of the persons concerned?

(iv) Electronic data under most jurisdictions is considered as being intangible. The law of some jurisdictions may only permit seizure of tangible material. In such cases, intangible data can only be obtained by seizing the physical medium (eg., data on diskette or other storage medium) on which the data is stored and found. Do your nation's laws provide for the seizure of intangible data without seizure of the physical medium which it is found?

(v) In some cases, the precise location of electronic data within a computer system may not be apparent. How specific must be the description in the judicial authority (eg. search warrant) of the place to be searched or the data to be seized?

[4] More information about the Netherlands hotline against child pornography on Internet can be found at: http://www.xs4all.nl/~meldpunt

(vi) In most jurisdictions, the scope of a warrant should be as narrow as possible. The precise location of the electronic data may not be immediately apparent at the time a warrant is sought, or even when law enforcement agents arrive at the scene. Does the law provide guidance on whether to seize the entire computer system, or merely one or more of its components? What practical criteria do law enforcement use to make this decision? How would this be done in practice?

(vii) Does your law obligate a suspect or a third person to provide access (including passwords) to a computer system that is the target of a lawful search? If not, what practical measures or tools can be employed by law enforcement to gain access?

(viii) Seizure of, or during the course of a search the shutting down of, an entire computer system may be extremely intrusive, and particularly burdensome to an ongoing business. What practical circumstances would justify seizing or shutting down a complete system rather than merely taking a copy of the data? Does the law provide for copying of relevant data as an alternative to seizure, and can the copy be regarded as admissible evidence? Would the law permit the seizure of the entire database for the purpose of subsequently identifying the relevant data? What practical means can be used to copy large volumes of data?

(ix) In the course of a search, law enforcement authorities may come across incriminating data related to the crime under investigation, but which was not originally specified within the scope of the warrant. Can this data be legally seized without obtaining another warrant?

(x) In the course of a search, law enforcement authorities may come across electronic data relating to a crime different from that which is under the current investigation. Can this data be legally seized without obtaining another warrant?

(xi) Does the law permit seizure of data, without a warrant, under exigent circumstances, such as when there is risk of erasure or destruction of data? Alternatively, are law enforcement agents able to secure the premises or computer system, pending the obtaining of a warrant?

(xii) In some cases, the data sought may be located on another computer system that is networked to the system currently being searched. Does the law permit an extension of the search into the connected system in order to search and seize relevant data within the scope of the warrant? Can the warrant include an authorisation to extend the search to the connected system? Alternatively, can law enforcement obtain a second warrant to extend the search from one system to the other?

(xiii) Are there any circumstances under which the law permits stored data to be obtained by means of a judicial order to deliver such data to law enforcement authorities, as opposed to the law enforcement authorities themselves searching and seizing it?

(a) Stored Transaction Data

(i) Records of service use, also known as transaction data, may be kept by some telecommunication carriers and internet service providers. Some carriers or ISPs may, for business or security purposes, retain such data for a period of time. In some jurisdictions, the cooperation of Internet service providers (ISPs) in identifying suspects may be obtained informally. Can this data be voluntarily provided to law enforcement agents by carriers and service providers? Does the law provide a means by which this data can be compulsorily obtained by law enforcement authorities?

(ii) Which types of transaction data does law enforcement require? Which types of transaction data do telecommunications carriers retain? For how long do the carriers or ISPs retain such data? Are there any laws or regulations which require them to retain such data, or to dispose of it after a certain period of time?

(b) Electronic communications

(i) Does the law permit law enforcement to collect current or future transaction data (including the source or destination of communications)? Can this authority for collection of current and future transaction data be achieved by satisfying legal conditions less onerous than that required to intercept the content of communications? What practical or technological means can be used to collect such data? Does law enforcement have the capability to undertake such techniques?

(ii) Even when one is able to determine the location from which a communication originates, identifying the human source of the communication may prove to be challenging. What legal and/or technological tools are available for this purpose?

(iii) How is the ability to collect such current or future transaction data affected if the communication crosses jurisdictional borders, including international borders?

(iv) Does the law permit interception of communications for the purpose of obtaining their content? Does the law permit this interception in respect of communications between computer systems or their components, as well as between persons? Does law enforcement have the practical capability to undertake such investigative techniques?

(v) In some cases, search or interception may be more efficiently and more effectively carried out by representatives of the telecommunications or ISP industry rather than law enforcement personnel. Does the law provide authority or obligation for private organizations or individuals to engage or assist in interception or search on behalf of the state? How does this affect the admissibility of the data as evidence in judicial proceedings? If there is no such authority or obligation, are there trained law enforcement personnel to undertake this task, and how would they do so?

(c) Analysis of data

(i) What legal, practical or technical means are available to preserve the data seized or intercepted in order to ensure its presentation and admissibility in judicial proceedings? What procedures should be followed?

(ii) If the data seized are encrypted, what legal, practical or technical means are available to allow law enforcement to decrypt data? Does law enforcement have legal authority to decrypt seized data using technical means? Can an order be sought from a judicial authority to compel decryption by the suspect or a third person? Can an order be sought to compel a suspect or a third person to hand over the encryption key or algorithm to law enforcement?

(d) Human rights and privacy safeguards

(i) Can a person to whom compulsory measures are applied, as above, challenge the lawfulness of such measures before a court, either before or after execution?

(ii) What legal protections exist for law enforcement agents who are undertaking a coercive investigative measure such as a search and seizure, or interception?

(iii) Which types of remedies may be ordered by a judicial authority?

(iv) How would such remedies be obtained or enforced in the context of a trans-border search?

(v) To what extent would legal protections or immunities apply to law enforcement from another country who are undertaking a trans-border search in your country?

This last question leads us into entirely new terrain.

B. Extra-Territorial Issues

One of the more significant aspects of computer-related crime is its global reach. While international offending is by no means a uniquely modern phenomenon, the global nature of cyberspace significantly enhances the ability of offenders to commit crimes in one country which will affect individuals in a variety of other countries. This poses great challenges for the detection, investigation and prosecution of offenders.

Two problems arise in relation to the prosecution of telecommunications offences which have an inter-jurisdictional aspect: first, the determination of where the offence occurred in order to decide which law to apply and, secondly, obtaining evidence and ensuring that the offender can be located and tried before a court. Both these questions raise complex legal problems of jurisdiction and extradition (see Lanham, Weinberg, Brown and Ryan 1987).

Even if one is able to decide which law is applicable, further difficulties may arise in applying that law. In a unitary jurisdiction, such as New Zealand, where there is one law and one law enforcement agency, determining and applying the applicable law is difficult enough. Criminal activities committed from across the globe, however, pose even greater problems. Sovereign governments are finding it difficult to exercise control over online behaviour at home, not to mention abroad. A resident of Chicago who falls victim to a telemarketing scam originating in Albania, for example, can expect little assistance from law enforcement agencies in either jurisdiction. As a result, regulation by territorially-based rules may prove to be inappropriate for these types of offences (Post 1995).

Extraterritorial law enforcement costs are also often prohibitive. The time, money and uncertainty required by international investigations, and if successful, extradition proceedings, can be so high as to preclude attention to all but the most serious offending. Moreover, the cooperation across international boundaries in furtherance of such enforcement usually requires a congruence of values and priorities which, despite prevailing trends towards globalization, exists only infrequently.

Other issues which may complicate investigation entail the logistics of search and seizure during real time, the sheer volume of material within which incriminating evidence may be contained, and the encryption of information, which may render it entirely inaccessible, or accessible only after a massive application of decryption technology.

If an online financial newsletter originating in the Bahamas contains fraudulent speculation about the prospects of a company whose shares are traded on the Australian Stock Exchange, where has the offence occurred?

Traditionally, the jurisdiction of courts was local. That is, courts could only entertain prosecutions in respect of offences committed against local laws where there existed a sufficient link between the offence and the jurisdiction in question. There is, however, always the possibility that legislatures will confer extraterritorial jurisdiction for some crimes. Some common examples include offences committed on the high seas, counterfeiting offences, crimes committed by members of the defence forces, and, recently in Australia, sexual relations between Australians and children overseas who are under 16 years of age.

In rare circumstances, a nation's laws may apply to acts committed overseas by foreign nationals. Recent war crimes prosecutions in Australia involved defendants resident elsewhere at the times the alleged offences were committed. These circumstances are, to say the least, most unusual. But in a shrinking world where the financial burdens of extradition are unlikely to decline, they may become more common.

To the extent that international telecommunications-related crime is amenable to international enforcement, it will require concerted international co-operation. Past performance in the context of other forms of criminality would suggest that this cooperation is unlikely to be forthcoming except in the relatively infrequent types of illegality where there is widespread international consensus about the activity in question (such as child pornography or fraud on a scale likely to destabilise financial markets), and about the desirability of suppressing it. In many instances, extradition is likely to be more cumbersome, the greater the cultural and ideological distance between the two parties.

Even so, this would assume a seamless world system of stable sovereign states; such a system does not exist today, nor is it likely to exist in our lifetime. Law enforcement and regulatory vacuums exist in some parts of the world, certainly in those settings where the state has effectively collapsed. Even where state power does exist in full force, the corruption of individual regimes can impede international cooperation.

What are some of the issues relating to cross-national investigations of computer crime?

Trans-border search and seizure

(i) Can investigative authorities in one country obtain, directly through an inter-connected computer system, data which exists abroad? Can this data be obtained from a publicly available source? Can data be obtained from private systems or data banks with the consent of third parties who have the right to access the data in the other country, without seeking judicial authority or permission from the other country?

(ii) Does the law of your country permit law enforcement agencies to undertake a trans-border search directly into another country, through an inter-connected computer system? Would your law permit them to do it if they had to break or compromise a password in the foreign country in order to obtain the data? If a transborder search occurs, should a notification be made to the state involved, or to the persons involved?

(iii) In the above circumstances (the two previous points), if the data being searched from abroad resides in your country, does your law permit foreign law enforcement agents to search and seize data in your country through the inter-connected system? If it is not contrary to law, would your country consider it to be contrary to public policy or a violation of national sovereignty?

Mutual legal assistance

(i) If your country requires that a foreign state only obtain data which resides in a computer system in your country by means of formal mutual legal assistance, does your country have legal and administrative mechanisms in place which would permit this to be obtained expeditiously? Are there legal tools which permit temporary seizure or preservation of data pending receipt and evaluation of the formal request? If your country is the requesting country, do you have legal and administrative mechanisms in place that would enable the request to be made expeditiously?

(ii) If legal authority is required from another jurisdiction in order to search, do you have legal and administrative mechanisms in place which would permit this to be obtained expeditiously?

Issues of transborder criminality aside, many law enforcement agencies as we know them, lack the capacity on their own to control computer related crime which occurs entirely within their own jurisdiction.

This arises from a number of factors, not the least of which is resource constraint. In most western industrial societies, police are being asked to do more with less. The broad sweep of the criminal law and the abundance of criminal activity means that police must often choose what matters to pursue and which to ignore.

Another fundamental issue, at least at the present historical moment, is the difficulty faced by police services around the world in retaining expert computer crime investigators. Much like the priesthood, policing was formerly a lifetime vocation. In many police services today, trained computer crime investigators must battle for the equipment which they regard as necessary to do their job. The development of expertise in forensic computing, moreover, may require a concentration and specialisation that precludes the development of the more general expertise required for advancement through the ranks. With the traditional high status areas of policing such as homicide investigation now joined by those of general management as the most prestigious jobs in law enforcement, prospects for upward mobility on the part of the computer crime investigator are thus limited.

At the same time, very attractive opportunities exist in the private sector for persons with forensic computing skills. A competent police officer may well be able to double or triple his or her salary in the private sector, whether working for one of the big multinational accounting firms or a large financial institution.

Whether this "brain drain" will continue indefinitely, or rather slow down as the supply of highly computer literate individuals in both public and private sectors catches up with demand, remains to be seen. For the time being, however, police will not be able to go it alone. They will remain dependent upon private and non-profit institutions to combat crime in cyberspace.

In general, this division of labour will include elements of self protection by prospective victims of telecommunications-related illegality; market-based commercial solutions; self regulatory initiatives by the targets of regulation; traditional law enforcement or regulatory intervention by the state; and third party "co-production" of surveillance by private individuals and citizens' groups.

Conclusion

Trans-national crime of a more conventional nature has proved to be a very difficult challenge for law enforcement. Computer-related crime poses even greater challenges. There may be differences between jurisdictions about whether or not the activity in question has occurred at all, whether it is criminal, who has committed it, who should investigate it and who should adjudicate and punish it.

There is a fundamental tension between the deregulatory imperative which characterises the world's advanced economies and the desire to control some of the darker corners of cyberspace.

There is a significant danger that premature regulatory interventions may not only fail to achieve their desired effect, but may also have a negative impact on the development of technology for the benefit of all. Over-regulation, or premature regulatory intervention may run the risk of chilling investment and innovation. Given the increasingly competitive nature of the global marketplace, governments may be forced to choose between paternalistic imperatives and those of commercial development and economic growth.

The challenge facing those who would minimise computer-related crime is to seek a balance which would allow a tolerable degree of illegality in return for creative exploitation of the technology. At this early stage of the technological revolution, it may be useful for individuals, interest groups and governments to articulate their preferences and let these serve as signals to the market. Markets may be able to provide more efficient solutions than state interventions.

To be sure, cyberspace is hardly the first or the only policy domain which lies beyond the control of any single nation state. International air traffic, the law of the sea, funds transfers, and such environmental considerations as ozone depletion and global warming, among others, have required concerted international efforts. One would expect that the development of international arrangements in response to telecommunications-related crime will occur in a manner not unlike those which have accompanied other extraterritorial issues, from drug trafficking, to nuclear testing to whaling. Whether the realm of telecommunications will be able to achieve a better record of success than these other enduring global issues remains to be seen.

Acknowledgements

This paper is based in part on research conducted in collaboration with Dr Russell G. Smith of the Australian Institute of Criminology.

In addition, the author wishes to acknowledge the contributions of Donald Piragoff of the Canadian Ministry of Justice, Professor Hendrick Kaspersson of the Free University of Amsterdam, and other members of the UN Special Expert Working Group to the development of the questions relating to search and seizure.

Opinions expressed in this paper are those of the author and not necessarily those of the Australian Government.

References

ASSOCIATED PRESS (1998) "First cyber terrorist action reported" Nando. Net. http://www.techserver.com/newsroom/ntn/info/050698/info9_25501_noframes.html (visited 4 January 2000)

BBC (1999) Nato under 'cyber attack' http://www.flora.org/flora.mai-not/10498 (visited 4 January 1999)

CREED, A (1999) Indonesian Govt Suspected In Irish ISP Hack Newsbytes February 21, 1999 http://www.ccurrents.com/newstoday/99/02/21/news8.html visited 10/01/00

DENNING, D. (1999) Information Warfare and Security. Boston: Addison Wesley.

EDWARDS, O. (1995) "Hackers from Hell" Forbes, 9 October: 182.

GOLD, Steve (1999) "BT Starts Switchboard Anti-Hacking Investigation" Jan 11 (Newsbytes) http://www.infowar.com/ visited 23/12/99.

GRANT, A., DAVID, F., and GRABOSKY, P. (1997) "Child Pornography in the Digital Age" Transnational Organized Crime, 3,4, 171-188.

HUNDLEY, R. and ANDERSON, R. (1995) "Emerging Challenge: Security and Safety in Cyberspace", IEEE Technology and Society Magazine, 14(4): 19-28.

LANHAM, D., WEINBERG, M., BROWN, K. E. and RYAN, G. (1987) Criminal Fraud. Sydney: Law Book Co. Ltd.

LITTMAN, J. The Watchman: The Twisted Life and Crimes of Serial Hacker Kevin Poulsen. Boston: Little Brown.

MEYER, M. and UNDERWOOD, A. (1994), "Crimes of the Net", Bulletin / Newsweek, November 15: 68-9.

NEWMAN, Keith (1998) "Phone Call Scams Skim off Millions" New Zealand Herald 20/08/98 http://www.infowar.com/ (Visited 23 December 1999)

POST, D. G. (1995), "Anarchy, State, and the Internet: An Essay on Law-Making in Cyberspace", Journal of ONLINE Law, art. 3.

RATHMELL, A (1997) Cyber-terrorism: The Shape of Future Conflict? Royal United Service Institute Journal (October, 40-46. http://www.kcl.ac.uk/orgs/icsa/rusi.htm#who (visited 21/12/99)

RYAN, M (1998) Knowledge Diplomacy: Global Competition and the Politics of Intellectual Property Wahsington: Brookings.

SCHIECK, M. (1995) "Combating Fraud in Cable and Telecommunications", IIC Communications Topics No. 13. London: International Institute of Communications.

SCHWARTAU, WINN (1994) Information Warfare: Chaos on the Electronic Superhighway. New York: Thunder's Mouth Press.

STOLL, CLIFFORD. (1991) The Cuckoo's Egg. London: Pan Books.

TENDLER, S. and NUTTALL, N. (1996), 'Hackers Leave Red-Faced Yard with $1.29m Bill', The Australian, 6 August: 37.

UNITED STATES, INFORMATION INFRASTRUCTURE TASK FORCE (1995) Intellectual Property and the National Information Infrastructure: Report of the Working Group on Intellectual Property Rights. (Bruce A. Lehman: Chair), Washington: US Patent and Trademark Office.

VENDITTO, G. 1996, "Safe Computing", Internet World, September: 48-58

WAHLERT, G. (1996) "Implications for Law Enforcement of the Move to a Cashless Society", 22-28 in Graycar A. and Grabosky P. N. (eds.), Money Laundering. Canberra: Australian Institute of Criminology.