VISITING EXPERTS' PAPERS

CRIME IN CYBERSPACE

*Peter Grabosky**

I. INTRODUCTION

It has almost become trite to suggest that we are entering an age as significant and profound in its impact as was the Industrial Revolution. The convergence of computing and communications has already affected most if not all of the major institutions of society. It has created unprecedented opportunities for education, health services, recreation, and commerce. Unfortunately, it has also created unprecedented opportunities for crime. Identifying these vulnerabilities, and mobilizing appropriate countermeasures, will be one of the great challenges of the next century. As we will observe, the challenge is so great that it defies the capacity of law enforcement alone to control. Consequently, new forms of policing, involving the harnessing of non-government resources, will become essential. Given the fact that cyberspace knows no boundaries, and that computer crime often transcends national frontiers, effective countermeasures will also require a degree of international co-operation which is without precedent.

II. VARIETIES OF COMPUTER 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.

* Director of Research, Australian Institute of Criminology, Australia

A. Theft of Information Services

Ever since the original "phreakers" of a quarter century ago attacked telephone systems out of curiosity, telecommunications services have been vulnerable to theft. From those whose motives were confined to simple mischief making, to those who have made theft of services a way of life and major criminal industry, those who steal services pose a significant challenge to carriers, service providers, and to the general public, who often bear the financial burden of fraud.

The market for stolen communications services is large. There are those who simply seek to avoid or to obtain a discount on the cost of a telephone call. There are others, such as illegal immigrants, who are unable to acquire legitimate information services without disclosing their identity and their status. There are others still who appropriate information services to conduct other illicit business with less risk of detection.

The means of stealing telecommunications services are diverse, and include the "cloning" of cellular phones, counterfeiting of telephone cards, and unauthorised access to an organization's telephone switchboard. In one case, hackers were reported to have obtained unauthorised access to the telephone facilities of Scotland Yard, and made US$1 million in phone calls.

B. Communications in Furtherance of Criminal Conspiracies

Modern information systems clearly provide an effective means by which offenders can communicate in order to plan

and execute their activities. There is evidence of information systems 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). Although the use of information facilities does not cause such illegal conduct to occur, it certainly enhances the speed and ease with which individuals may act together to plan and to execute criminal activity.

C. Information Piracy/ Counterfeiting/Forgery

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. Arguably, the speed and accuracy with which copies of works may now be made has been dramatically enhanced by such modern technology as online information networks. Copyright infringement may occur quickly and without difficulty, and may be carried out by anyone capable of using the Internet. 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.

As broadband services continue to become available with text, graphics, sound and video information being freely accessible via cable modems, the potential for copyright infringement involving such works will be enhanced enormously. Already in the United States it is possible to download compact disks and feature films from the Internet.

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. Information 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. In one recent case, a student composed a sadistic fantasy and sent it out over the Internet. He used the name of a fellow student as the story's victim, and was initially charged with communicating a threat, although this was later withdrawn.

The rich diversity in thresholds of tolerance around the world, combined with the global reach of information, make this a particularly difficult regulatory challenge. What is offensive to authorities in the People's Republic of China, might be welcome in overseas Tibetan communities. Materials offensive to religious leaders in Iran may fail to raise an eyebrow elsewhere.

E. Electronic Money Laundering

For some time now, electronic funds transfers have assisted in concealing and moving the proceeds of crime. Emerging technologies will greatly assist in concealing the origin of ill-gotten gains. 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 information technology.

With the emergence and proliferation of various technologies of electronic commerce, one can easily envisage how traditional countermeasures against money laundering 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.

F. Electronic Vandalism and Terrorism

As never before, western industrial society is dependent upon complex data processing and information systems. Damage to, or interference with, any of these systems can lead to catastrophic consequences. A recent United States government study estimated that some 250,000 separate attempts to penetrate United States defence installations had occurred during the previous year. Not all of these are attributable to harmless curiosity. Defence planners around the world are investing substantially in information warfare as a means of disrupting the information technology infrastructure of defence systems. Whether motivated by curiosity, vindictiveness or greed, electronic intruders cause inconvenience at best, and have the potential for inflicting massive harm.

G. Sales and Investment Fraud

The use of the telephone for fraudulent sales pitches, deceptive charitable solicitations, or bogus investment overtures is a billion dollar a year industry in the United States. The intensification of commercial activity in the United States and globally, combined with emerging communications technologies, would seem to heighten the risk of sales fraud. Already evidence is emerging of fraudulent sales and investment offers having been communicated over computer networks and Bulletin Boards. Further developments in electronic marketing will provide new opportunities for the unscrupulous and new risks for the unwitting.

H. Illegal Interception of Information

Developments in information 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, information interception has increasing applications. Here again, technological developments create new vulnerabilities. In New York, for example, two individuals recently used a sophisticated scanning device to pick up some 80,000 cellular telephone numbers from motorists who drove past their Brooklyn apartment. Had the two not been arrested, they could have used the information to create cloned mobile telephones which could have resulted in up to $100 million in illegal calls being made. 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.

I. Electronic Funds Transfer Fraud

The proliferation of electronic funds transfer systems will enhance the risk that such transactions may be intercepted and diverted. Existing systems such as Automated Teller Machines, and Electronic Funds Transfer at Point of Sale technologies have already been the targets of fraudulent activity. The development of stored value cards or smart cards, super

smart cards and optical memory cards will no doubt invite some individuals to apply their talents to the challenge of electronic counterfeiting and overcoming security access systems. Just as the simple telephone card can be reprogrammed, smart cards are vulnerable to re-engineering. Credit card details can be captured and used by unauthorised persons. The transfer of funds from home between accounts and in payment of transactions will also create vulnerabilities in terms of theft and fraud and the widescale development of electronic money for use on the Internet will lead to further opportunities for crime. What has for the past quarter century been loosely described as "computer fraud" will have numerous new manifestations.

The above forms of illegality 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 information services and use them for purposes of vandalism, fraud, or in furtherance of a criminal conspiracy.

Communication of some forms of prohibited material (such as that relating to the manufacture of drugs or explosive devices) may itself entail criminal conspiracy. Even legitimate telemarketing may be regarded as intrusive and offensive to some recipients. Intrusions and interceptions for the purposes of industrial espionage may also be accompanied by theft of intellectual property.

In addition, 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.

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.

III. THE TRANSNATIONAL IMPLICATIONS OF CRIME IN CYBERSPACE

International crime of a more conventional nature has proved to be a very difficult challenge for law enforcement. Computer and telecommunications related crime poses even greater challenges. There may be a lack of agreement between authorities in different jurisdictions about whether or not the activity in question is criminal at all, who has committed it, whether in fact it has been committed, who has been victimised because of it, who should investigate it, and who should adjudicate and punish it. 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?

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.

IV. COUNTERMEASURES

It has long been recognized that the criminal justice system is a very imperfect means of social control, and that effective crime prevention requires the contribution of families, schools, and many other institutions of civil society. This is no less the case with crime in cyberspace than it is with crime in the streets.

It will be immediately apparent that the detection, investigation and prosecution of all of the above forms of criminality pose formidable challenges. Crime in the digital age can be committed by an individual in one jurisdiction against a victim or victims on the other side of the globe. The control of cyber-crime lies beyond the capacity of any one agency. What principles can we articulate to assist us in controlling computer crime?

A. Emphasize Prevention

It is a great deal more difficult to pursue an online offender to the ends of the earth than to prevent the offence in the first place. The trite homily that "prevention is better than cure" is nowhere more appropriate than in cyberspace. It applies no less to high technology crime than it does to residential burglary. Just as one would be most unwise to leave one's house unlocked when heading off to work in the morning, so too is it foolish to leave one's information systems accessible to unauthorised persons.

B. Self Defence Should Be the First Line of Defence

The first step in the prevention of online crime is to raise awareness on the part of prospective victims to the risks which they face. Individuals and institutions should be made aware of the potential consequences of an attack on their information assets, and of the basic precautionary measures which they should take. Those businesses who stand to gain the most from electronic commerce have the greatest interest in developing secure payment systems. Technologies of computer security, to be discussed below, can provide significant protection against various forms of computer crime. There are other, "low technology" measures which should not be overlooked. Perhaps foremost among these is staff selection. Surveys of businesses reveal that one's own staff often pose a greater threat to one's information assets than do so called "outsiders". Disgruntled employees and former employees constitute a significant risk. Suffice to say that great care should be taken when engaging and disengaging staff.

C. Non-governmental Resources Should Be Harnessed Whenever Possible

Given the resource constraints which most governments face, it is desirable to enlist the assistance of private sector and community interests in the prevention and detection of computer-related crime. Market forces will generate powerful influences in furtherance of electronic crime control. Given the immense fortunes which stand to be made by those who develop secure processes for electronic commerce, they hardly need any prompting from government. In some sectors, there are ample commercial incentives which can operate in the furtherance of cyber-crime prevention. Information security promises to become one of the growth industries of the coming century. Some of the new developments in information security which have begun to emerge include technologies of authentication. The simple password for access to a computer system, vulnerable to theft or determination by other means, is being complemented or succeeded altogether by biometric authentication methods such as retinal imaging and voice or finger printing.

Detection of unauthorised access to or use of computer systems can be facilitated by such technologies as artificial intelligence and neural networking, which can identify anomalous patterns of use according to time of day, and keystroke patterns.

Issues of objectionable content can be addressed at the individual level by blocking and filtering software, by which parents or teachers can prevent children's access to certain types of sites. Selective consumption of internet content can be further assisted by classification schemes such as the Platform for Internet Content Selection.

The energies of private individuals can also be enlisted in furtherance of security and prosperity in cyberspace. A wide range of websites, under governmental or non-governmental auspices, invite private citizens to report suspected illegal conduct on the internet to authorities. Some such as the Cyber Angels, invite disclosures of all kinds, while others tend to specialize in particular areas, such as fraud or child pornography. What might be described as an "Electronic Neighbourhood Watch" enhances the capacitity to detect some forms of electronic illegality.

The are other areas in which the state might arguably take a subordinate role to the individual. Consider violations of copyright or theft of intellectual property. In situations where civil remedies might be available to the victim, it is arguably more appropriate for the individual to secure their own rights than to rely upon the state to act on one's behalf. One could, of course, envisage circumstances where a wider state role may be justified—for example when the perpetrator in question is engaged in other criminal activity, or when the theft in question has wider economic ramifications. But conferring rights upon the individual and providing the individual with the means of enforcing these rights may be appropriate in some circumstances.

In extreme cases, some would take the law into their own hands. The metaphor of cyberspace as a frontier is not entirely inapposite. There are vigilantes in cyberspace. In some instances, self-help by victims of telecommunications related crime may itself entail illegality. "Counter-hacking" by private citizens or by government agencies has been suggested as one way of responding to illegal intrusions. A group calling itself 'Ethical Hackers Against Pedophilia' have threatened to disable the computers of those whom they find dealing in digital child pornography.

A radical response to the problem of software piracy is to make use of so-called Logic Bombs which are installed into programs. When activated through an act of unauthorised copying, the malicious code would destroy the copied data and even damage other software or hardware belonging to the offender. The potential for such practices to result in liability for criminal damage, however, makes their use problematic.

D. Enhancing the Capacity of Law Enforcement

The continuing uptake of digital technology around the world means that law enforcement agencies will be required to keep abreast of rapidly developing technologies. This will entail training in new investigative techniques. As new technologies are exploited by criminals, it becomes even more important for law enforcement not to be left behind. This is a significant challenge, given the emerging trend for skilled investigators to be "poached" by the private sector. The collaboration of law enforcement with

specialized expertise residing in the private sector will be a common feature in years to come.

One may also expect to see the use of fairly aggressive investigative methods in cyberspace. Even the domestic policing of telecommunications-related illegality may require measures which go beyond traditional law enforcement tactics. The technologies of encryption and anonymity noted above are invoked to justify aggressive investigative methods such as covert facilitation, more commonly referred to as "stings". In mid-1995 for example, the FBI charged an adult male who arranged over the Internet to meet what he thought was a 14 year old girl at a motel. The Internet contact was in fact an FBI agent. The accused was targeted because of his history of sex offences involving minors. Similar tactics have been directed at those who traffic in pornographic material, as well as perpetrators of telemarketing fraud. Law enforcement officers can easily pose on-line as prospective consumers of pornography. Laws will vary across jurisdictions with regard to the defence of entrapment, and the extent to which an offence was encouraged or suggested by police.

E. The Imperative of International Cooperation

The global nature of cyberspace necessitates the development of new strategies to combat criminal activity which can originate from the other side of the world. At present, if I, in Australia, were gullible enough to fall victim to a fraudulent investment scheme originating in Albania, I suspect that I could count on very little help from authorities in either jurisdiction. But transnational electronic crime seems destined only to increase.

The basic approach to overcoming the transnational issues of crime in cyberspace lies in developing cooperation between nations. This is more easily said than done, given the significant differences in legal systems, values and priorities around the world.

Enlisting the assistance of overseas authorities is not an automatic process, and often requires pre-existing agreements relating to formal mutual assistance in criminal matters.[1] Nevertheless, there are numerous examples of successful measures.

1. Unilateral Action

Some governments may take unilateral action against their citizens or residents who commit criminal offenses on foreign soil. Two of the most familiar examples in Australia are prosecutions for engaging in sexual activity with children, and for war crimes alleged to have been committed in World War Two. However in many cases, this may still require the co-operation of a foreign government in obtaining evidence and possibly in extraditing the offender.

2. Bilateral Agreements

The mobility of criminal offenders in a shrinking world has increased the need for arrangements to facilitate the apprehension and repatriation of those who seek to evade the law by fleeing to another jurisdiction. The most common mechanism for this is extradition, which is done pursuant to a treaty or other formal

[1] Following recent amendments to the Mutual Assistance in Criminal Matters Act 1987, Australia may now grant assistance in criminal matters to any country. Bilateral mutual assistance treaties are currently in force with 18 nations. A further four treaties have been signed, but are not yet in force.

arrangement between two nations.[2] Australia was the originator of 33 and the recipient of 37 extradition requests pending at 30 June 1997.

Since 1985, Australia has adopted a "no evidence" approach as the preferred basis for international extraditions. The earlier approach required the production of a prima facie brief against the person sought, which effectively required foreign jurisdictions to produce evidence which accorded with Australia's technical rules of admissibility. This was particularly difficult for civil law countries. The new approach is reflected in most of Australia's modern extradition treaties and has generally facilitated cooperation between Australia and other jurisdictions.

Some jurisdictions seek to prosecute offences committed abroad by foreign nationals against their own citizens. The United States, for example, can seek extradition of alleged terrorists who have offended against citizens of the United States while abroad. Extradition is by no means an automatic matter, as the recent experience of Australian fugitive Christopher Skase illustrates. Moreover, other impediments exist. Some nations will not extradite their own citizens under any circumstances. Australia, as a matter of policy, will not extradite a fugitive who would face execution in the jurisdiction seeking his or her return. Those jurisdictions which do practice capital punishment may waive the death penalty in order to obtain the extradition of a fugitive.

There are circumstances in which, as an alternative to extradition, a nation may prosecute a citizen for offences committed in, and against the laws of, a foreign jurisdiction. Australia, for example, may prosecute Australian citizens for offences committed on foreign soil, provided the relevant conduct would have been an offence under Australian law had it occurred within Australia. This process is only available within Australia in circumstances where extradition has been refused on the sole ground that the person was an Australian citizen at the time of the offence, and only if the Commonwealth Attorney-General is satisfied that the requesting State would have refused extradition of its nationals in corresponding circumstances. There are no recorded cases of such prosecutions within Australia.

In addition to extradition, a variety of arrangements may be put in place to facilitate cooperation between nations in the location and collection of evidence in furtherance of criminal investigation. Mutual assistance treaties, as they are called, provide a legal basis for authorities in country "A" to obtain evidence for criminal investigations at the request of authorities from country "B". Instruments of this kind cover a range of assistance including:

- the identification and location of persons;
- the service of documents;
- the obtaining of evidence, articles and documents;
- the execution of search and seizure

[2] By the end of 1997, Australia had signed bilateral extradition treaties with 32 countries. Twenty nine of these were in force. A further 64 jurisdictions were covered by the London Extradition Scheme, which provides for the rendition of fugitive offenders among members of the Commonwealth of Nations. A special extradition relationship exists with New Zealand. Australian extradition laws have been applied to seven additional countries without a treaty. Australia has succeeded to extradition treaties entered by the United Kindom with 21 countries in the late 19th and early 20th centuries.

requests; and
- assistance in relation to proceeds of crime.

Australia was the originator of 162 mutual assistance requests, and the recipient of 130 requests by other nations, which were pending at 30 June 1997.

The Mutual Assistance in Criminal Matters Act 1987 was amended in March 1997 to provide for "passive" application of the Act to all foreign countries, rather than requiring the Act to be specifically applied to particular countries by regulation. This enables assistance to be requested and provided much more expeditiously than was previously the case.

In addition, the posting of law enforcement personnel overseas can facilitate the development of informal networks which can help expedite response to the various requests which may arise from time to time. Formal agreements are essential, but there is often no substitute for interpersonal contact. The Australian Federal Police has 29 liaison officers stationed in 13 nations around the world. In addition to serving Australia's needs, the AFP and Australian consular staff are able to help overseas governmental authorities check on the probity of prospective investors from Australia. AFP liaison officers may also assist their hosts in the training of law enforcement personnel and in the exchange of intelligence.

Steps taken following the G-8 Birmingham meeting in May 1998 for nations to designate liaison offices, which will be on call on a 24 hour basis, illustrates the need for prompt concerted responses to the problem of transnational digital crime.

V. CONCLUSION

It has become trite to suggest that the world is a shrinking place. On the one hand, this shrinking is highly beneficial. People around the world now enjoy economic, cultural and recreational opportunities which were previously not accessible. On the other hand, the rapid mobility of people, money, information, ideas and commodities generally, has provided new opportunities for crime, and new challenges for law enforcement agencies. Linkages between events and institutions at home and abroad are inevitable, and will proliferate. This will require unprecedented cooperation between nations, and will undoubtebly generate tensions arising from differences in national values. Even within nations, tensions between such values as privacy and the imperatives of enforcement will be high on the public agenda. New organizational forms will emerge to combat new manifestations of criminality. The 21st century will be nothing if not interesting.