Digital Crime in the Twenty-First Century[1]

P. N. Grabosky and Russell G. Smith

At the beginning of the twenty-first century, the convergence of computing and communications technologies has altered considerably the way in which industrialized communities function. It has created untold benefits for education, delivery of health services, recreation, and commerce, and changed considerably the nature of modern workplaces and patterns of employment. Unfortunately, it has also created unprecedented opportunities for crime (see Grabosky and Smith, 1998). Identifying these vulnerabilities, and mobilizing appropriate countermeasures, will be one of the great challenges facing us as the new millennium unfolds.

This article 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 digital 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. Given the fact that cyberspace knows no boundaries, and that computer crime often transcends national frontiers, effective countermeasures will also require a substantial degree of international cooperation.

P.N. Grabosky, Director of Research, and Russell G. Smith, Senior Research Analyst, Australian Institute of Criminology, GPO Box 2944, Canberra, ACT, 2601, Australia (Email: Peter.Grabosky@aic.gov.au)

We begin by discussing ten of the latest forms of digital crime — that is, crime that involves information systems as instruments or as targets of illegality. By digital, we refer to the fact that information systems simply operate by reducing data to streams of "1s" and "0s." Almost every type of information is thus able to be transmitted across telecommunications networks connected either by wires or by means of radio communications.

Varieties of Digital Crime

The variety of criminal activity that 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 entirely new forms of illegality altogether. These forms of crime are not necessarily mutually exclusive, nor is the following list exhaustive.

Theft of Telecommunications Services

The "phone phreakers" of three decades ago set a precedent for what has become a major criminal industry. The market for stolen communications services is now large. There are those who simply seek to avoid or to obtain a discount on the cost of a telephone call while 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 illicit business with less risk of detection. All pose a significant challenge to carriers, service providers, and to the general public — who often bear the financial burden of fraud.

The means of stealing telecommunications services are diverse, and include the "cloning" of cellular phones, and the counterfeiting of telephone cards. It may also entail gaining unauthorized access to an organization's telephone switchboard (PBX). By gaining access to a PBX, individuals or criminal organizations 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 five per cent 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).

Communications in Furtherance of Criminal Conspiracies

Just as legitimate organizations in the private and public sectors rely upon information systems for communications and record keeping, so too are the activities of criminal organizations enhanced by technology. There is evidence of telecommunications equipment being used to facilitate organized 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 also 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 organization, 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 organization. Although knowledge is confined to that conduct that has been the target of successful police investigation, there appear to have been a number of networks established that have extended across national borders, 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 fourteen nations ranging from Europe, through 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.

Information Piracy/Counterfeiting/Forgery

Digital technology permits perfect reproduction and easy dissemination of print, graphics, sound, and multimedia combinations. It is now possible, for example, to download music from the latest compact disks and feature films from the Internet. The temptation to reproduce copyright material for personal use, for sale at a lower price, or indeed, for free distribution, has proven irresistible to many. According to the *Straits Times* (8 November 1999), a copy of the most recent James Bond Film *The World Is Not Enough*, was available free on the Internet before its official release. This, and similar incidents, have caused considerable concern to owners of copyright material. 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.

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.

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.

Dissemination of Offensive Materials

Content considered by some to be objectionable exists in abundance in cyberspace. This includes, among much else, sexually explicit materials (including child pornography, as we have seen above), 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. Although 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 five 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.

Digital Extortion

Computer networks may also be used in carrying out criminal extortion. *The Sunday Times* (London) reported in 1996, that over forty financial institutions in the United Kingdom and the United States had been attacked electronically during 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*, 2 June 1996). The article cited four incidents between 1993 and 1995 in which a total of £42.5 million were paid by senior executives of the organizations 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 (ISP) 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. Cooperation between United States 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).

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, that 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 that 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).

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).

Although this potential has yet to be realized, a number of individuals and protest groups have hacked the official web pages of various governmental and commercial organizations (Rathmell, 1997).[2] This may also operate in reverse. Early in 1999, an organized hacking incident was apparently directed at a server that hosted the Internet domain for East Timor, which at the time was seeking its independence from Indonesia (Creed, 1999).

Defense planners around the world are investing substantially in information warfare means of disrupting the information technology infrastructure of defense systems (Stix, 1995).[3] 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 (British Broadcasting Corporation, 1999).

Electronic Sales and Investment Fraud

As electronic commerce becomes more prevalent, the application of digital technology to fraudulent business endeavors 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 possibilities such as coconut farming, the sale and leaseback of automatic teller machines, and worldwide telephone lotteries (Cella and Stark, 1997, 837–44). 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).

Illegal Interception of Digital Information

Developments also provide new opportunities for electronic eavesdropping. From activities as time-honored 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 (*West Australian*, 9 July 1996, 47). Organized criminals in Amsterdam have obtained unauthorized access to information systems of the Dutch police.

The electromagnetic signals emitted by a computer may themselves be intercepted. Cables may act as broadcast antennas. In many jurisdictions, 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 organization attacked the communications system of the Amsterdam Police. The hackers succeeded in gaining police operational intelligence, and in disrupting police communications (Rathmell, 1997).

Electronic Funds Transfer Crime

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 and 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 unauthorized 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 for the past quarter century has been loosely described as "computer fraud" will have numerous new manifestations.

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).

Common Themes and Issues

Secrecy and Anonymity

A number of common themes and issues are present in each of the forms of digital crime described above. The first concerns the way in which technologies can conceal the content of communications and disguise the identity of users. Technologies of encryption, for example, can limit access by law enforcement personnel 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).

In addition to victims of digital crime being reluctant to report their victimization to the authorities, 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. Finally, technology has greatly facilitated so-called identity-related economic crime in which offenders fabricate documents through the use of desktop publishing equipment to misrepresent their own identity or make use of another's identity for illegitimate purposes (Smith, 1999).

Motivations

Given the diversity of digital crime, it is not surprising that the various types of behavior 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 digital 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 the commission of digital crime have proliferated. 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 digital 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 that flow from new technologies, while minimizing the downside. A merchant could scrutinize every credit card transaction 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 that reduce the opportunity to commit digital crime. Given that so much digital crime depends upon unauthorized 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 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 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 fingerprint or voice recognition technology and retinal imaging, which greatly enhance the difficulty of obtaining unauthorized access to information systems. Virus detectors can identify and block malicious computer code, while 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

Much digital crime takes place simply because of 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, as well as 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 digital 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 mobilized. 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 into 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 ISPs specializing 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. Sub-contractors 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 is the Simon Wiesenthal Center, whose "CyberWatch Hotline"[4] invites notification of anti–Semitic and racist material.

Citizen co-production can also 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 Internet

Providers (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.[5]

The policing of terrestrial space is now very much a pluralistic endeavor, and so too is the policing of cyberspace. Responsibilities for the control of digital 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 in terrestrial space two millennia ago, the first line of defense will be self-defense — in other words, minding one's own store.

Extra-Territorial Issues

One of the more significant aspects of digital crime is its global reach. Although 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 that 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 offenses that have an inter-jurisdictional aspect: first, determining where the offense 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 behavior 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 offenses (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 that, despite prevailing trends towards globalization, exists only infrequently.

Other issues that 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 offense occurred?

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

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 digital crime than it is with traditional forms. It will be immediately apparent that the detection, investigation, and prosecution of all of the above forms of digital crime 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 cybercrime lies beyond the capacity of any one agency. What principles can we articulate to assist us in controlling computer crime?

The Importance of Prevention

It is a great deal more difficult to pursue an online offender to the ends of the earth than to prevent the offense 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 unauthorized persons.

Effective digital crime prevention entails carrying out risk analyses of information systems and the creation of effective policies and procedures to protect them from damage or misuse. In the workplace, for example, policies should be created on the use of office telecommunications and computing facilities for personal purposes and whether staff should be able to encrypt communications in order to prevent them from being read by others. Efforts are also needed to ensure that software and disks are regularly checked for viruses and malicious code that could damage systems and the information that they contain.

The prevention of digital crime may also entail the use of electronic monitoring of usage. For two decades now, call accounting systems, which produce call-logs for each telephone extension, systematically compile data on the length, cost, and destination of each call. Now, new "Internet Manager" software can create custom reports on Internet usage by individual employees. Similarly, the use of sophisticated neural networks are able to analyze computer usage to ensure that unusual transactions or usage that might involve criminality are able to be promptly detected and dealt with. In making use of such electronic crime prevention technologies, however, considerations of privacy and confidentiality need to be considered and respected.

The Role of Self Help

Another key principle in the prevention of digital crime is the need to raise awareness on the part of prospective victims to the risks that 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 that they should take. Those agencies that stand to gain the most from electronic commerce have the greatest interest in developing secure payments systems. Technologies of computer security can provide significant protection against various forms of computer crime. But there are other, "low-technology" measures that 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 it to say that great care should be taken when engaging and disengaging staff, or in outsourcing IT activities to the private sector. Similarly, systems and the information contained therein should be backed up regularly. This will not prevent an attack, but it will reduce the risk of irretrievable loss of or damage to data in the event of an attack or system failure.

The Use of Non-governmental Resources

More generally, given the resource constraints that most governments face, it is desirable to enlist the assistance of private sector and community interests in the prevention and detection of digital crime.

Market forces will generate powerful influences in furtherance of electronic crime control. Given the immense fortunes that 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 that can operate in furtherance of digital crime prevention. Information security promises to become one of the growth industries of this century. Some of the new developments in information security that 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 unauthorized access to or use of computer systems can be facilitated by such technologies as artificial intelligence, 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 systems administrators can prevent employees' access to certain types of sites. Simple software can track web sites visited and the amount of time spent at each site. Internet Manager software enables a systems administrator to develop a custom blocking list that could deny access to pages containing certain specified keywords. Other software called Surfwatch can develop customized access categories. When an employee clicks for a page, the software matches the user ID with the content allowable for the assigned category, then either loads the requested page, or advises the user that her request has been denied. The software logs denied requests for later inspection by management. Some software packages can also measure and record the bandwith consumed by Internet applications.

In extreme cases, some would take the law into their own hands. The metaphor of cyberspace as a frontier is not entirely inappropriate. There are vigilantes in cyberspace. In some instances, self-help by victims of digital 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. Public sector managers would be well advised to avoid becoming the initiator or the target of counter hacking.

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 unauthorized copying, the malicious code would destroy the copied data and even damage other software or hardware belonging to the offender.

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.

And it will be important for public sector managers to develop close ties with law enforcement, to report suspected illegality to them, as well to provide them with assistance when required. The police and the institutions that they serve in both public and private sectors should be familiar with each others' needs.

The Importance of International Cooperation

As already mentioned, the global nature of cyberspace necessitates the development of new strategies to combat criminal activity that can originate from the other side of the world. The basic approach to overcoming the transnational issues of digital crime 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.[6] Nevertheless, there are numerous examples of successful measures, and the web of mutual assistance is being woven ever more tightly.

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 that 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. Linkages between events and institutions at home and abroad are inevitable, and will inevitably proliferate. This will require unprecedented cooperation between nations, and will inevitably generate tensions arising from differences in national values. Even within nations, tensions between such values as privacy and the imperatives of law enforcement will be high on the public agenda. New organizational forms will emerge to combat new manifestations of criminality.

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 minimize digital crime is to seek a balance that would allow a tolerable degree of illegality in return for creative exploitation of the technology. Even 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 then be able to provide appropriate responses that governments are unwilling or unable to achieve. Digital crime is bound to increase as the new century unfolds. By making effective use of traditional crime control measures coupled with some sophisticated technological solutions, it may, however, be able to be kept within manageable limits.

Notes

1. This article updates and expands some material previously published as Grabosky, P. N., and Smith, R.G., 1997, "Telecommunications and Crime: Regulatory Dilemmas," *Law and Policy*, 19, 3, 317–41. Opinions expressed in this article are those of the authors and not necessarily those of the Australian Institute of Criminology or the Australian Government.

2. See also <http://www.2600.com/hacked–pages/> (visited 4 January 2000).

3. See also the website of the Institute for the Advanced Study of Information Warfare (IASIW) <http://www.psycom.net/iwar.1.html> (visited 4 May 2000).

4. See <http://www.wiesenthal.com/watch/index.html> (visited 4 May 2000).

5. More information about the Netherlands hotline against child pornography on Internet can be found at <http://www.meldpunt.org/meldpunt-eng.htm> (visited 4 May 2000).

6. 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.

References

Associated Press. (1998). First Cyber Terrorist Action Reported. <*http://www.techserver.com/newsroom/ntn/info/050698/info9_25501_noframes.html*> (visited 4 January 2000).

British Broadcasting Corporation. (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*, 21 February. <*http://www.ccurrents.com/newstoday/99/02/21/news8.html*> (visited 10 January 2000).

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

Edwards, O. (1995). Hackers from Hell. *Forbes*, 9 October, p. 182.

Gold, S. (1999). BT Starts Switchboard Anti-Hacking Investigation. *Newsbytes*, 11 January. <http://www.infowar.com/> (visited 23 December 1999).

Grabosky, P. N., and Smith, R. G. (1998). *Crime in the Digital Age: Controlling Telecommunications and Cyberspace Illegalities*, Leichhardt: Federation Press/New Brunswick: Transaction Publishers.

Grant, A., David, F., and Grabosky, P. (1997). Child Pornography in the Digital Age. *Transnational Organized Crime*, 3 (4), 171–88.

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.

Littman, J. (1997). *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*, 15 November, pp. 68–9.

Miller, G., and Maharaj, D. (1999). N. Hollywood man charged in 1st cyber-stalking case. *Los Angeles Times*, 22 January. <http://www.cs.csubak.edu/~donna/news/crime.html#stalking> (visited 12 June 1999).

Newman, K. (1998). Phone Call Scams Skim Off Millions. *New Zealand Herald*, 20 August. <*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, pp. 40–6 <*http://www.kcl.ac.uk/orgs/icsa/rusi.htm#who*> (visited 21 December 1999).

Ryan, M. (1998). *Knowledge Diplomacy: Global Competition and the Politics of Intellectual Property*. Washington, DC: Brookings.

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

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

Smith, R. G. (1999). Identity-Related Economic Crime: Risks and Countermeasures. In *Trends and Issues in Crime and Criminal Justice*, No. 129. Canberra: Australian Institute of Criminology.

Stoll, C. (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, p. 37.

Two on Phone Scam Counts. (1996).*West Australian*, 9 July, p. 47.

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, DC: United States Patent and Trademark Office.

Venditto, G. (1996). Safe Computing. *Internet World*, September, pp. 48–58.

Wahlert, G. (1996). Implications for Law Enforcement of the Move to a Cashless Society. In Graycar, A., and Grabosky, P. N. (eds.). *Money Laundering* (pp. 22–8). Canberra: Australian Institute of Criminology.

About the Contributors

Shawn M. Clankie is a frequent writer on issues of names and the law. In 1999, he received a Ph.D. in Linguistics from the University of Hawai'i at Mānoa. His dissertation research presented a theory to account for generic change in brand names. He is currently on the faculty of the Institute of Language and Culture Studies at Hokkaido University in Sapporo, Japan.

Edward Cline is an independent scholar and novelist.

Russell Eisenman, Ph.D., is a faculty member at the University of Texas and a prolific author.

P. N. Grabosky, Ph.D., is Director of Research at the Australian Institute of Criminology.

Anthony J. Graybosch is professor of philosophy at California State University–Chico. His areas of interest are American philosophy, ethics and the family, and rock and blues.

Robert Hauptman edits the *Journal of Information Ethics.*

Jack Hibbard, Ph.D., is a faculty member at St. Cloud State University.

Steve McKinzie is currently the Social Science Liaison Librarian at Dickinson College, Carlisle, Pennsylvania. McKinzie tries to review and write for the library field as much as he can, believing that librarians generally are not as controversial or polemical as they ought to be.

Russell G. Smith, Ph.D., is senior research analyst at the Australian Institute of Criminology.

Cassandra Van Buren, Ph.D., is an assistant professor in the Communication Department at Trinity University in San Antonio, Texas. Her research and teaching center on communication, technology, and culture.