AUSTRALIAN INSTITUTE OF CRIMINOLOGY

trends & issues

in crime and criminal justice

No. 59

Crime and Telecommunications

P.N. Grabosky, Russell G. Smith, Paul Wright

Telecommunications technology has begun to provide criminal opportunities of unprecedented scope and dimension. The revolution in information technology which we are currently experiencing is perhaps the most significant development of our time. Recent and anticipated changes in telecommunications technology in light of the connectivity of communications and computing are truly breathtaking, and have already had significant impacts 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. Their capacity for more efficient operation has increased as well. Along with this greater capacity, however, comes greater vulnerability. This Trends and Issues paper summarises a current research project at the Australian Institute of Criminology which is exploring risks and countermeasures relating to the use of telecommunications as the instrument and/or as the target of crime.

Adam Graycar
Director

The overall objectives of the telecommunications and crime project at the Australian Institute of Criminology are to identify:

- current and emerging forms of criminality involving telecommunications systems as the instruments and / or the targets of criminal activity;
- organisational and regulatory shortcomings which facilitate the commission of the illegality in question;
- difficulties which tend to arise in the detection, investigation, and prosecution of the illegal activity;
- typical outcomes of the legal process; and
- countermeasures which will minimise future risk of the illegality in question, without inflicting collateral harm.

Our work will conclude with a discussion of the most appropriate regulatory configuration to address the various forms of telecommunications-related 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, regulatory and market solutions.

The project will also consider issues arising from the global reach of telecommunications. Figuratively speaking, telecommunications systems have made the world a smaller place and few can now ignore the fact that financial decisions made in London or Tokyo quickly reverberate around the world, having their impact locally. Celebrity images manufactured in Hollywood become the new icons in Russia; pornographic images crafted in Denmark are accessible to 15-year-olds in Australia. The corresponding potential for trans-jurisdictional offending will pose formidable challenges to the successful

August 1996

ISSN 0817-8542
ISBN 0 642 24021 3

Australian Institute
of Criminology
GPO Box 2944
Canberra ACT 2601
Australia

Tel: 06 260 9200
Fax: 06 260 9201
http://www.aic.gov.au

mobilisation of effective countermeasures.

Types of Crime

The variety of criminal activity which can be committed with or against telecommunications 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 involving telecommunications systems as instruments and / or as targets is the subject of our inquiry. These are not necessarily mutually exclusive, nor is the list complete. They do, however, represent the primary areas of concern for policy makers.

Theft of telecommunications services

Ever since the original "phreakers" of a quarter-century ago attacked telecommunications 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 a major criminal industry, those who steal services pose a significant challenge to telecommunications carriers, service providers, and to the general public, who often bear the financial burden of fraud.

The market for stolen telecommunications services is large indeed. 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 telecommunications services without disclosing their identity and their status. There are others still who appropriate telecommunications services to conduct other illicit business with less risk of detection. Across the world, immense sums of money are lost by the victims of such illegality. Substantial sums are also incurred in preventing, detecting and prosecuting offences.

Criminal conspiracies

The essential element of a criminal conspiracy consists of one or more individuals entering into an agreement to commit a criminal offence. Modern telecommunications facilities clearly provide an effective means by which such agreements may be reached. The emergence of networks which are inaccessible to law enforcement agencies through the use of private key encryption and the technology of high speed data transfer, can greatly enhance the capacity of sophisticated criminal organisations to engage in their preferred activities. 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).

Theft of intellectual property

Billions of dollars in sales and royalties are lost each year because of copyright infringements. The speed and accuracy with which accurate copies of works may now be made has been dramatically enhanced by such modern technology as online telecommunications networks. Copyright infringement may occur quickly and without difficulty, and may be carried out by anyone capable of using the Internet. Rapid development and widespread accessibility of emerging multi-media technologies are creating new horizons of opportunity for intellectual property pirates.

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 harrassing, threatening or intrusive communications, from the traditional obscene phone call to its contemporary manifestation in "cyber-stalking", in which persistent messages are sent to an unwilling recipient.

Electronic money laundering

For some time now, electronic funds transfers have assisted in concealing and in moving the proceeds of crime. Emerging technologies may greatly assist in concealing the origin of ill-gotten gains (Wahlert 1996). 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 traditional countermeasures against money laundering may soon be of limited value.

Electronic vandalism

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 (Hundley & Anderson 1995). In November 1988, a computer program was introduced into the Internet which quickly impeded the operation of some 6000 computers across the United States. Estimated costs of diagnoses

and system maintenance exceeded several million dollars. United States defence installations have been popular targets (US GAO 1996). Defence planners around the world are investing substantially in information warfare means of disrupting the information technology infrastructure of defence systems (Stix 1995). University computing systems have also been targetted by virtue of their accessibility to inquisitive and technically competent young people. On at least one occasion, an attack on a computer used to prepare weather forecasts led to the loss of a ship at sea (Cheswick & Bellovin 1994, p. 15).

Telemarketing fraud

The use of the telephone for fraudulent sales pitches, phony 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 we have seen the emergence of fraudulent sales and investment pitches on the Internet. Developments in electronic marketing will provide new opportunities for the unscrupulous and new risks for the incautious.

Illegal interception

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. Aided by simple scanning hardware, an individual can sit at home and monitor nearby cordless telephone communications. Although electromagnetic signals emitted by a computer may themselves be intercepted, existing law does not prevent the remote monitoring of computer radiation.

Electronic funds transfer fraud

The proliferation of electronic funds transfers 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 may prove vulnerable to reverse engineering. The transfer of funds from home between accounts and in payment of transactions will create vulnerabilities in terms of theft and fraud and the widescale development of electronic money for use on the Internet will also lead to opportunities for crime.

The Enforcement Challenge

The size of the problem

Unfortunately, telecommunications-related crimes, unlike bank robberies or fatal motor vehicle accidents, tend to defy quantification. Some of the most deftly perpetrated offences with or against telecommunications 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 has been provided by Stoll (1991) whose pursuit of a US$0.75 accounting error in a computer account led to the unravelling of an international espionage ring.

Even qualitative descriptions can be illusory. Many people, regardless of their calling, are inclined to accentuate their accomplishments. Telecommunications criminals are no exception. While some thrive on anonymity, others seek notoriety. This latter group often embroider their activities. There is a significant gap between what they do, what they say they do, and what they think they do. Law enforcement agencies, on the other hand, have been known to overstate the magnitude of a problem in order to justify maintaining or enhancing their resource base. Other actors who arguably have commercial incentives to accentuate the gravity of a problem include the security industry and the news media.

Beyond the aforementioned reluctance of victims to report, the technologies of secrecy and anonymity such as encryption of data, often make detection of the offender extremely difficult. Those who seek to mask their identity 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, while others may never be discovered. Considerable time may elapse before the activation of a virus, or between the insertion of a logic bomb and its detonation.

Extraterritorial issues

One of the more significant aspects of telecommunications-related crime is its global reach. While international offending is by no means a uniquely modern phe-

nomenon, the globalisation of telecommunications significantly enhances one's vulnerability to offences committed from abroad. It has become trite to suggest that we are living in a world without borders. This may have greater truth for offenders than for law enforcement agencies. As such, it poses profound implications for detection, investigation and prosecution of offenders.

Two problems arise in relation to the prosecution of telecommunications offences which have an international aspect: first, the determination of where the offence occurred in order to decide which jurisdiction's 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.

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. In federal systems, such as Australia, Canada, or the United States, however, extraterritorial law enforcement becomes more difficult.

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. 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 often prohibitive. Moreover, the cooperation across international boundaries in furtherance of such enforcement usually requires a congruence of values and priorities which, despite prevailing trends towards globalisation, exists only infrequently.

Images, ideas, and practices regarded as perfectly acceptable in one place may be regarded as heinous in another. The authorities in one jurisdiction who are untroubled by electronic depictions of nudity, the works of Salman Rushdie, or the virtues of Tibetan independence, are unlikely to expend much time and effort in assisting the authorities in those jurisdictions who are offended by such content.

It has, for example, taken three decades to achieve a modest consensus about the merits of international mutual assistance in furtherance of combating drug traffic and money laundering. Even in those nations characterised by agreement in principle, the actual implementation can be difficult (Nadelmann 1993). Similar problems exist in relation to international copyright regulation and banking arrangements.

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 and expensive cryptoanalytic effort.

Additional problems are reflected in the difficulty of exercising national sovereignty over capital and information flows. Jurisdictional issues may arise from transborder online transmission. If an online financial newsletter originating in Albania contains fraudulent speculation about the prospects of a company whose shares are traded on the Australian Stock Exchange, where has the offence occurred?

The Range of Countermeasures

Given the difficulties noted above, it seems appropriate to think in terms of a variety of institutions and instruments which can be brought to bear on the illegalities in question. The varied nature of telecommunications related illegality defies a single policy solution. Indeed, each of the basic forms of illegality described above is sufficiently complex that, if a solution exists at all, it is likely to entail a combination of instruments. In general, this combination will include elements of self-protection by prospective victims of telecommunications related illegality; market-based commercial solutions; self-regulatory initatives 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.

Self-help

Given the limited capacity of governments to control telecommunications-related crime, the first line of defence lies in the exercise of prudent behaviour by prospective victims. Just as the first step in the control of burglary is to lock one's doors and windows, so too the basic principles of information security should be honoured.

Whether the risk in question entails hacking, fraud, or unwilling exposure to objectionable content, individuals and organisations can take positive steps to protect themselves. The exercise of simple prudence, such as by the use of procedures which restrict access to computer systems, will suffice in many cases. This has led to computer security becoming one of the world's growth industries. In addition to more rigorous management practices and the introduction of more sophisticated password and verification procedures, new technologies such as biometric security devices and anomaly detection programs help enhance the security of computer systems.

After the event, the first line of redress may lie with victims too. The usual avenue of recourse in

cases of intellectual property infringement or defamation is the civil courts in an action for damages. Recently, a university lecturer in Western Australia was awarded substantial damages after having been the subject of unflattering comment on the Internet (*Rindos v. Hardwick*, Supreme Court of Western Australia, 31 March 1994). In those instances where service providers may be aware of the injurious nature of the content, they too may be liable. In these circumstances, legal risk helps to leverage an extra degree of scrutiny which might not otherwise occur.

Commercial solutions

The market itself may deliver products which will assist individual initiatives to defend against telecommunications illegality. Consider, for example, the problem of access to offensive materials on the Internet. A rich variety of commercial software exists with which to block access to certain sites. In addition, a market is currently emerging for service providers specialising in content suitable for family consumption, guaranteed to be free of sex, violence, and vilification.

In addition, there is likely to be an increasing market for damage control services in the aftermath of an attack on telecommunications systems. Victimized organisations may well be more concerned about enhancing system security and restoring normal operations than about mobilising the law and in the process, attracting public attention to their vulnerability. The development of computer emergency response teams (CERTS), industry funded and arms length from law enforcement, helps meet this need.

The commercial potential of the Internet, which may well become the dominant medium of commerce in our lifetime, has not been lost on entrepreneurs around the world. Commercially developed technologies will seek to safeguard the trust which is required as the basis for commerce, and minimise the risk of abuse.

Sometimes, problems can be converted into solutions. Consider the computer virus, the bane of systems operators worldwide. As a countermeasure against software piracy, a "logic bomb" could be incorporated in a commercial software product, designed to be activated when copied for the second time.

Market forces may also generate second-order controlling influences. As large organisations 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 insureds.

Self-regulation

A modicum of self-regulation may also be exercised by telecommunications carriers and service providers. While the sheer volume of traffic may preclude scrutiny of all content, many service providers now require signed undertakings as a condition of service that the user shall refrain from illegal activity, as well as from a range of lesser breaches of protocol. Breaches of such undertakings may result in termination of services.

Faced with the threat of heavy-handed attempts by government to impose regulation on Internet communications, various industry groups are developing codes of practice, to reduce the likelihood of some of the more egregious abuses of cyberspace.

Citizen co-production

Citizen concern about the availability of undesirable content has given rise to the private monitoring and surveillance of cyberspace. Two of the more prominent organisations involved in such surveillance are the Simon Wiesenthal Center, whose CyberWatch Hotline invites notification of anti-semitic and racist material, and the Guardian Angels, whose Cyber Angels division recruits volunteers to "patrol" cyberspace in search of a range of illegal and objectionable content. These include images of child pornography, vilification and harassment, fraudulent schemes, software piracy, developments in computer viruses and content pertaining to terrorism, and the manufacture of explosives. Information gathered from volunteers is forwarded to law enforcement authorities in the case of criminal activity, and to service providers where breaches of codes of conduct are involved. Public interest groups also encourage websites registering as "child safe" or "child friendly", to enable parents to employ commercially available software to guide children's access.

Traditional enforcement

Law enforcement is inhibited by many of the fiscal, technological and extraterritorial considerations noted above. Nevertheless, procedures and practices are being developed, and increasingly shared, for the investigation of telecommunications-related crime. Difficulties are such, however, that conventional enforcement seems destined to be reserved for only the most serious breaches.

Despite the challenges which exist in cyberspace, the information superhighway has become a boon to law enforcement. Although its potential has yet to be realised, the use of technology for general public relations, for the communication of basic information for crime prevention, and for

the exchange of information in furtherance of criminal investigation may be expected to increase dramatically in years ahead. Already photographs displayed on the Internet have led to the arrest of persons on the FBI's most wanted list.

Unintended Consequences

The terrain of telecommunications-related illegality includes conflicts and contradictions: many apparent solutions turn out to be double-edged swords which produce unintended consequences, in some cases worse than the underlying problem. As in other areas of regulation and public policy, one must take care that a particular defence against telecommunications-related illegality does not create more harm than it is intended to address (Grabosky 1995).

Similarly, there exists what might be termed the "forbidden fruit effect". Official attempts to block access to a given site can inspire the emergence of so-called "mirror sites" in more permissive jurisdictions, which serve to proliferate points of access to the material in question. Attempts to suppress Canadian sites which promulgated neo-Nazi propaganda, and arguably prejudicial information about an ongoing criminal trial, were singularly unsuccessful in this regard.

Conclusion

International crime of a more conventional nature has proven to be a difficult challenge for law enforcement. Telecommunications-related crime poses even greater challenges. There may be a lack of agreement about whether or not the activity in question is criminal at all, whether in fact it has been committed, who has committed it, who has been victimised because of 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 the less pleasant aspects of telecommunications. Nevertheless, a case can be made for the deregulatory ethos to prevail, at least for the time being.

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. Overregulation, 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 telecommunications 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.

Telecommunications 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 issues 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 cooperative efforts to combat telecommunications crime will achieve a better record of success than has been realised in these other enduring global issues remains to be seen.

ACKNOWLEDGMENT

This research was funded in part by a grant from the Telstra Fund for Social and Policy Research in Telecommunications. Opinions expressed are those of the authors, and not necessarily those of the Australian Government.

References

Cheswick, W.R. & Bellovin, S.M. 1994, *Firewalls & Internet Security*, Addison-Wesley, Reading, MA.

Grabosky, P. 1995, "Counterproductive regulation", *International Journal of the Sociology of Law*, vol. 23, pp. 347-69.

Hundley, R. & Anderson, R. 1995, "Emerging challenge: Security and safety in cyberspace", *IEEE Technology and Society Magazine*, vol. 14, no. 4, pp. 19-28.

Nadelmann, E. 1993, *Cops across Borders: The Internationalization of U.S. Criminal Law Enforcement*, Pennsylvania State University Press, University Park.

Post, David G. 1995, "Anarchy, State and the Internet: An essay on law-making in cyberspace", 1995 J.Online L, art.3, http://warthog.cc.wm.edu/law/publications/jol

Stix, G. 1995, "Fighting future wars", *Scientific American*, vol. 273, no. 6, pp. 74-80.

Stoll, C. 1991, *The Cuckoo's Egg*, Pan Books, London.

United States, General Accounting Office 1996, *Information Security: Computer Attacks at Department of Defense Pose Increasing Risks*, GAO/AIMD-96-84, 22 May.

Wahlert, G. 1996, "Implications for law enforcement of the move to a cashless society", in *Money Laundering*, eds A. Graycar & P.N. Grabosky, Research and Public Policy Series No. 2, Australian Institute of Criminology, Canberra, pp. 22-8.

Dr Peter Grabosky is Director of Research, Dr Russell G. Smith is Senior Research Officer, and Mr Paul Wright is a Research Officer who was on leave from the WA Police Service at the Australian Institute of Criminology.

Submissions for consideration for the Trends and Issues series should be forwarded to:
Dr Adam Graycar, Director
Australian Institute of Criminology
GPO Box 2944
Canberra ACT 2601 Australia