AUSTRALIAN INSTITUTE OF CRIMINOLOGY

trends & issues

in crime and criminal justice

No.93

Criminal Exploitation of New Technologies

Russell G. Smith

Recent technological developments have created a wide range of novel methods by which individuals may break the law. Technology not only facilitates the commission of many existing forms of illegal conduct but also represents a target for some new forms of illegality which are directed at technological products and services themselves. In addition, some technological changes have created entirely new types of crime. This paper reviews some of the principal ways in which technological developments over the last few years have established new opportunities for the commission of crime, and how future developments may have like consequences. Armed with this knowledge, legislators and law enforcement personnel may take immediate action to prevent some of the more egregious technologically-based crimes of the future.

Adam Graycar
Director

Throughout history, individuals have made use of contemporary technological developments to enable them to commit both property crimes and crimes of personal violence. In the twelfth century, for example, crossbows were developed to improve the operation and efficiency of traditional longbows, thus providing a powerful weapon initially for military use but subsequently for use in robbery and murder (Hewitt 1996, p. 158). Crossbows were used not only to propel deadly quarrels (feathered bolts), but were also adapted to discharge pellets and stones. The crossbow continues to be a silent and efficient device for killing and is now classified as a prohibited weapon (*see*, for example, *Weapons Act 1991* (ACT) Schedule 3, item 14).

Financial offenders have also relied heavily on technological developments. In Roman times, for example, counterfeiting of currency made use of the same technologies that were used to make legitimate coins and notes. Often it was only the ineptitude of the counterfeiters who inadvertently included spelling mistakes and figurative errors on their coins which led to their detection.

Without providing recipes for the construction of illegal devices, substances and weapons, and, hopefully, without providing ideas to stimulate the imagination of those with criminal propensities, this paper examines the most recent technological developments which have been used to carry out illegal conduct. Some predictions will also be made as to the technological advances which offenders in the future may rely upon and how best to guard against their improper use.

Technologies of Violence

Crimes of violence, particularly serious offences such as robbery and murder, invariably involve the use of weapons, some of more refined construction than others. A diverse range of weapons are either prohibited or closely regulated by legislation throughout Australia. Some weapons were originally devised for legitimate purposes, such as spear guns for underwater fishing. Others, such as riding crops which contain a stiletto, or fountain pens capable

July 1998

ISSN 0817-8542
ISBN 0 642 24074 4

Australian Institute
of Criminology
GPO Box 2944
Canberra ACT 2601
Australia

Tel: 02 6260 9200
Fax: 02 6260 9201

For subscription information together with a complete list of the papers in the Trends and Issues in Crime and Criminal Justice series, visit the AIC web site at:

http://www.aic.gov.au
or send an email to:
aicpress@aic.gov.au

of discharging gas or bullets, were obviously invented for more sinister uses. Prohibited weapons such as the Farallon Shark Dart, which is designed to expel harmful gases on contact, or the Saunders "Falcon" Hunting Sling, a sophisticated catapult, have the capability of inflicting serious injuries if directed at people. Table 1 sets out data on the extent to which weapons were used in various types of offence in Australia during 1996.

Between 1995 and 1996, there was an 11 per cent increase in the use of weapons, and a 14 per cent increase in the use of firearms in recorded murders in Australia, although eleven per cent of the murder victims in 1996 related to a single incident in Port Arthur, Tasmania in which 35 people lost their lives through the use of firearms (ABS 1998, pp. 351-2).

Individual State and Territory police statistics provide more specific information concerning the type of weapons used. In Victoria, in 1996-97, for example, weapons were recorded as having been associated with 3847 offences, which is an increase of 48 per cent over the 2594 offences involving weapons in 1995-96. Table 2 sets out the extent to which different forms of weapons were used over the last three years.

Although small in number, the largest increase took place in the use of syringes, increasing from 30 offences in 1994-95 to 94 offences in 1996-97. This is a clear example of offenders making use of one technological development, originally designed for legitimate therapeutic purposes, but now adapted for violent purposes.

Developments in the manufacture of firearms have enhanced their power and range considerably and rapid-fire weapons are now able to deliver substantial numbers of bullets with devastating consequences. It is for this reason that self-loading firearms have been prohibited from use in Australia, except for restricted official purposes.

Technological developments have also enabled the manufacture of realistic replica firearms, which may be used to threaten individuals and to perpetrate acts of violence and robbery in public places.

Table 1: *Number and percentage of recorded crimes in which weapons were used in Australia in 1996*

	Weapons*		Firearms		None		
Offence Category	*N*	*(%)*	*N*	*(%)*	*N*	*(%)*	*(Total %)*
Assault	10 676	(9.4)	629	(0.6)	102 230	(90.0)	100.0
Robbery	4 652	(28.4)	1 565	(9.6)	10 129	(62.0)	100.0
Sexual Assault	253	(1.8)	19	(0.1)	14 122	(98.1)	100.0
Attempted Murder	159	(48.0)	100	(30.2)	72	(21.8)	100.0
Murder	142	(45.7)	98	(31.5)	71	(22.8)	100.0
Kidnapping / Abduction	45	(9.4)	26	(5.4)	408	(85.2)	100.0
Manslaughter	8	(21.6)	2	(5.4)	27	(73.0)	100.0

Source*:* Derived from Australian Bureau of Statistics (1997, pp. 27-85)
* All categories of weapon excluding firearms.

Electricity has also been used in a number of novel ways for the infliction of harm and injury including electrically-charged streams of water and electromagnetic fields capable of being directed at people.

The development of military technologies which have produced smaller and more deadly weapons has created a threat where such weapons fall into the hands of offenders, particularly terrorists (*see* Dobson & Payne 1982). In addition, the proliferation of both civil and military-based nuclear technologies has created the threat that these may be used by organised terrorist groups. The Internet has also provided an expansive advertising medium through which individuals are able to obtain some of these weapons or the technological skills necessary to create such weapons illegally. Although the illegal use in Australia of bombs and explosives is not of the same scale as in certain overseas countries, the Australian Bomb Data Centre nonetheless processed more than 400 reports on Australian and overseas incidents relating to the illegal use of explosives, and dispatched 153 bomb safety packages during 1996-97 (AFP 1997, p. 41). The use of explosives in international terrorist activities has also changed in recent years as terrorists have moved away from using compact, concealable bombs to attack aircraft to using bombs with enormous explosive force to attack office buildings (Leader 1997).

Technologies of Transportation

The modern motor car has provided opportunities for individuals to engage in a wide range of motoring offences, particularly those related to the use of excessive speed, or driving whilst intoxicated which often result in fatalities. The latest Australian Population Survey Monitor, for example, found that

Table 2: *Weapons used in Victorian offences 1994-97*

	% of Recorded Offences			% Change
Type of Weapon	*1994-95*	*1995-96*	*1996-97*	*1995-97*
Knife	34.9	37.3	40.8	+16.9
Other	22.6	22.5	19.0	-15.9
Firearm	17.6	16.1	16.0	-9.1
Bat / Bar	10.9	11.0	11.4	+4.6
Bottle	6.8	5.8	6.3	-7.4
Syringe	0.8	1.5	2.4	+200.0
Vehicle	3.5	2.4	2.4	-31.4
Axe / Tomahawk	1.5	1.0	0.9	-40.0
Explosive	1.4	2.3	0.7	-50.0

Source*:* Victoria Police 1997, p.14.

86 per cent of Australians aged eighteen years and over had driven a motor vehicle in the previous twelve months, and of these, 13 per cent believed that they had always or most of the time exceeded the speed limit by 10 km per hour, while 10 per cent believed that they had sometimes exceeded the 0.05 per cent blood alcohol limit while driving (ABS 1998). In 1995-96, 339 offences of driving causing death and 131 768 offences of theft of a motor vehicle were reported to the police in Australia (Mukherjee et al. 1997, p. 2).

Motor cars have also created an environment and culture in which acts of so-called "road rage" may occur in which individuals use motor cars to stalk or to harass other road users. In addition to their traditional use as "getaway cars", motor vehicles have been used to facilitate theft by so-called "ram raiding" in which stolen vehicles are driven into locked building entrances or windows in order to gain entry for criminal purposes.

The extensive reliance on air travel throughout the world has provided opportunities for aircraft hijacking and other forms of extortion and terrorism in which threats of violence directed at the large number of passengers carried on modern aircraft are used as a means of extracting funds or policy changes from companies or governments. Terrorist hijacking and bombing of aircraft, frequent occurrences in the 1980s, have declined in recent years although terrorists have since directed their attention to other forms of transportation such as suicide bus bombings and train derailments as well as making use of car and truck bombs to attack city buildings (Johnson 1997, Leader 1997).

Finally, the reliance of modern transportation systems on satellite and computer-based technologies has provided offenders with a ready target for acts of extortion or mass destruction. Whole communities may be held to ransom if transportation system computers such as those which control railway signals or aircraft flight paths are interfered with.

Computer-Based Technologies

Perhaps the most profound technological developments which have taken place in recent years have involved computer and telecommunications systems. These information systems have provided opportunities for the commission of an extensive range of illegal acts (*see* Grabosky & Smith 1998).

Table 3 sets out responses received in a recent survey of 159 large Australian organisations when representatives of each organisation were asked which of the specified forms of computer-related crime would increasingly have an impact on their organisation in the next five years.

Of the organisations surveyed, 54 per cent had either suffered from some form of unauthorised use of computers or were unaware of whether or not they had a problem. Four per cent of those surveyed had experienced more than fifty-one separate incidents, with 6 per cent experiencing losses of more than $100 000.

In another study which sought to forecast the future nature of high-technology crime, a group of experts from traditional law enforcement backgrounds and a group of computer offenders both agreed that criminal activity in the future will include attacks on computer systems via telecommunications networks and the use of computers to commit crimes of fraud and data manipulation, such as counterfeiting, financial fraud and software piracy (Coutorie 1995, p. 26).

Some of the specific ways in which computer-based technologies have been, and are being used illegally include the following.

Computer-based systems have been used to carry out a wide range of illegal surveillance activities. In addition to listening devices and telephone interception technologies, simple audio-visual devices have been used to carry out corporate espionage and surveillance of business competitors, while electro-magnetic impulses generated by computers have been intercepted and information obtained in breach of privacy and confidentiality laws.

Computers have been used to steal funds transmitted electronically between banks, merchants and consumers since

Table 3: *Computer crime vulnerabilities of the future*

Type of Computer Crime	Number of Respondents
Hacking or system intrusion	114
Misuse of telecommunications services	90
Greater use of encryption	76
Use of malicious code	54
Theft	53
Intellectual property offences	49
Fraud	46
Increase in potential for virtual crimes	30
Shift from conventional crimes	24
Use of false identities	23
Information warfare	21
Emergence of "black" information market	17
E-cash theft and counterfeiting	14
Forgery	12
Virtual company crime	11
Electronic extortion	11
Emergence of organised crime groups	9
Money laundering	6
Others	2

Source: Office of Strategic Crime Assessments and Victoria Police 1997.

electronic funds transfer systems were first developed. Recent payment systems involving stored value "smart" cards and electronic cash will be vulnerable to manipulation and fraud when security measures are compromised electronically. Even the most sophisticated systems being devised for electronic commerce, such as digital signatures which make use of public key cryptography, may be compromised if private keys are stolen or other access controls circumvented.

Desktop publishing technologies which enable documents to be scanned electronically and copies made and altered digitally, have provided extensive opportunities for counterfeiting and forgery of documents and the creation of false identities for use in various forms of commercial crime and fraud. In Victoria, for example, an offender opened forty-two separate bank accounts making use of false identification documents. Each account made use of a different false identity created by the offender using desktop publishing equipment. Forty-one false birth certificates were produced along with forty-one false student identification cards as well as a driver's licence. In addition to the false bank accounts, the offender was able to register a business name, make withdrawals from cheque accounts, obtain Medicare refunds and defraud various retailers (Victoria Police, Major Fraud Group 1998, personal communication).

Telecommunications systems also represent attractive targets for offenders who seek to obtain telephone services or online computer services without incurring fees. Frauds which make use of telephones and the Internet have greatly enhanced the problem of telemarketing crime and other forms of false and deceptive advertising.

Computers have also been used to commit various offences against the person such as Internet stalking and online sexual harassment as well as the transmission of obscene and objectionable materials over telecommunications networks. Computers have the potential greatly to facilitate communication among paedophiles as well as the transmission of child pornography.

Computers are also being used to disguise the proceeds of crime through on-line money laundering transactions employing electronic funds transfer systems. In addition, computers are being used to facilitate the theft of intellectual property, particularly copyright in computer software and audio-visual materials.

Technology now permits individuals involved in criminal conspiracies and organised crime to conduct their activities with reduced chances of detection by legitimate law enforcement and national security agencies. Cloned mobile telephones, for example, permit offenders to communicate without the need to engage a legitimate, traceable telephone service while encryption software permits data to be transmitted with little opportunity for surveillance by law enforcement agencies for use in subsequent criminal prosecutions. Even legally obtained, pre-paid, anonymous mobile telephone accounts provide opportunities for offenders to communicate without having to disclose their identities to the service provider.

Since the advent of extensive computer networks which connect millions of users worldwide, there exists a real and substantial possibility of the removal of and interference with confidential and personal information held by government and private agencies. Crimes involving breach of privacy and improper disclosure of confidential information will be a significant concern in the future.

Medical & Scienific Technologies

Medical technological developments have created opportunities for various new forms of criminality. New offences involving reproductive technologies, for example, such as illegal surrogacy arrangements, human cloning, unlawful killing through the withdrawal of life support and theft of human tissue and organs have all arisen through the development of new medical technologies.

Telemedicine, or the use of communication technologies in the diagnosis and treatment of patients, also provides opportunities for illegal and unprofessional conduct by health care providers. Apart from breach of confidentiality through the improper electronic dissemination of patient records, there is the possibility that health care providers may commit fraud relating to the provision of services as well as in connection with reimbursement of fees from government and private health care funds (Smith 1997).

Pharmacological substances, particularly those which have hallucinogenic effects, have been used in the contravention of laws relating to their possession, use and supply, while the illegal manufacture and dilution of drugs of addiction has involved both individual as well as complex organisational offenders.

The availability of chemical weapons and toxic gases, often devised for military use, has provided offenders, particularly terrorists, with new means of inflicting harm upon large sectors of the population with little chance of detection. Various chemical agents have been used against people since the first use of chlorine in World War I. These include blood agents such as hydrogen cyanide, choking agents such as phosgene, blistering agents such as mustard gas, and nerve agents such as tabun, soman and sarin. The most serious instance of this in recent years involved the release of sarin nerve gas on the Tokyo underground rail system on 20 March 1995 by the Japanese Aum Shrinri Kyo cult in which eleven people were killed and 100 admitted to hospital (Lewis 1997).

Intentional contamination of food and food products has also relied heavily on technological methods. In the United States in March 1982, for example, seven people died after ingesting the analgesic Tylenol which had been deliberately contaminated with cyanide, an incident which was repeated in that country in February 1986 (*Weekend Australian*, 15 February 1997, p. 23). In 1984, the members of an Oregon cult poisoned local residents using homemade salmonella.

Chemicals have also been used to facilitate the commission of sexual offences in recent years. In the United States, for example, tranquillising drugs have been slipped into the drinks of female university students in order to increase their vulnerability to rape. Although by no means a new way of carrying out such an offence, its incidence seems to be increasing, at least in some parts of the United States.

Illegitimate Use of Crime Control Technologies

Just as technology has improved the ability of law enforcement and security agencies to prevent and to control crime (*see* Grabosky 1998), so has it enabled offenders to avoid the effects of those same crime prevention achievements. Security measures such as surveillance devices, computer access systems, motor vehicle remote alarm devices, motor vehicle speed detection instruments and alcohol and drug testing systems have all been circumvented through the application of illegal technologies. Offenders have thus been able to defeat many of the technological systems designed to prevent illegal conduct and have, at the same time, committed new offences of defeating legitimate security measures.

Various non-lethal technologies designed by legitimate law enforcement agencies to restrain offenders such as nets, foams, adhesives, sound, light, chemical and electrical devices and substances may be used by offenders for illegitimate purposes to immobilise victims or law enforcement and security personnel themselves. There is a need, therefore, for such instruments to be manufactured and kept securely by those who use them for lawful purposes.

Control Strategies

Often new technologies are created without consideration being given to their potential for illegitimate use. Technological developments designed for military use, sometimes create enduring problems when used improperly in civilian contexts. The development of gun powder is the most striking example of this in the past, and the development of computers may well provide the twenty-first century's counterpart. Arguably, those involved in the development of new technologies should devote at least some of their time and budget to ensuring that they are not providing offenders of the future with new means of committing crimes, or adding to the risk of injury or death when crimes employing those technologies are carried out.

In the absence of such foresight, the question remains as to how technologies of crime may be controlled. Control strategies will generally seek to restrict the availability of the raw materials used to manufacture devices and weapons, to restrict the availability of those devices and weapons themselves, or to restrict their possession and use by certain categories of individuals.

Restricting the availability of precursors

Imposing controls on the availability of precursors, or the raw materials used in the manufacture of illegal devices, substances and weapons, seems to provide a workable response. Keeping secure stocks of white plastic used in the manufacture of credit cards, for example, is one way of preventing plastic card counterfeiting, while various nations now have stringent controls on the availability of chemicals used in the illegal manufacture of narcotic drugs. In 1995-96, for example, seizures of acetic anhydride prevented up to 120 tons or one billion street doses of heroin from being manufactured (Jayasuriya 1998).

Similarly, international controls have been imposed on precursors which may be used to manufacture biological and chemical weapons (*see* the Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxic Weapons and of their Destruction (ratified by Australia on 10 April 1972) and supplemented by the Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on their Destruction which came into force on 29 April 1997). International controls now exist, for example, on the availability of basic chemicals such as phosphorous trichloride and thionyl chloride which may be used in the construction of chemical weapons. In Australia, Commonwealth legislation creates specific offences relating to the development, production and stockpiling of biological and chemical weapons as well as weapons of mass destruction (*Crimes (Biological Weapons) Act 1976* (Cwlth), *Chemical Weapons (Prohibition) Act 1994* (Cwlth), *Weapons of Mass Destruction (Prevention of Proliferation) Act 1995* (Cwlth)).

Unfortunately, despite the most extensive security measures, black markets will inevitably be created for most substances used in the creation of illegal devices, substances and weapons. An added limitation associated with controlling the availability of precursors, is that often raw materials exist in the international marketplace, making their exclusion from Australia a difficult problem for the Australian Customs Service and the Australian Federal Police alike,

particularly since the advent of online marketing and commerce. Inter-agency cooperation is needed both nationally and internationally to identify and to prevent the illegal trade in prohibited materials.

Restricting availability of new technologies

Restricting the availability of technological devices and weapons has been attempted as a regulatory strategy throughout history. Crossbows were, for example, prohibited by Papal decree as being unfit for Christian warfare in 1139. In more recent times in Australia we have seen the resurgence of legal prohibitions relating to certain categories of firearm. Between 10 May 1996 and 30 September 1997, for example, the owners of 640 401 firearms which were declared to be illegal under new uniform laws enacted throughout Australia, were collectively paid over $300 million in compensation for handing them in to the authorities (Australian Firearms Buyback 1998). It is the view of those who support such initiatives that restricting the availability of the most dangerous firearms will prevent incidents of mass violence involving such weapons from taking place.

Legal prohibitions can, however, only eradicate illegitimate use to a limited extent. There is always the possibility of displacement effects in which legally available "substitute weapons" will be used instead of illegal ones (Harding 1983). Internationally, prohibitions on the creation of mass weapons of destruction have been difficult to enforce through the use of political and diplomatic measures.

Restricting possession and use

Attempts may also be made to restrict certain individuals from using technological devices in the commission of crime. Certain categories of person (for example minors) are already prohibited from possessing or using particular types of weapons, and disqualification from driving has been an effective sanction to deal with those who commit serious motoring offences. In the future, perhaps, those who have committed crimes using computers should also be prohibited from using similar such technologies. This has already been tried in the United States in the case of Kevin Lee Poulsen who, when released in July 1996 from a five-year term of imprisonment for computer hacking, was required to comply with a parole order preventing him from possessing computer equipment or working with computer equipment without the permission of his probation officer for a period of three years (Morello 1996).

What may be preferable is for those who develop new technologies to contemplate at the outset the potential for illegitimate use which they are providing. In order to do this, it will be necessary for manufacturers and designers of new technologies to predict how they may be put to illegal use. Understanding how the most sophisticated offenders are able to carry out their plans, is, arguably, an essential first step in preventing technology-based crime from taking place. The expected benefits of new developments, thus need to be balanced against any negative consequences which they may entail. Prevention is, in this sense, a more effective strategy to adopt than attempting to restrict the availability and use of technologies for illegitimate purposes once they have become publicly available.

References

Australian Bureau of Statistics 1997, *Recorded Crime*, Australia 1996, ABS Catalogue No. 4510.0, AGPS, Canberra.

———— 1998, *Yearbook Australia*, ABS Catalogue No. 1301.0, AGPS, Canberra.

Australian Federal Police 1997, *Annual Report 1996-97*, AFP, Canberra.

Australian Firearms Buyback 1998, Internet Home Page http://www.gun.law.gov.au.

Coutorie, L. E. 1995, "The future of high-technology crime: A parallel Delphi study", *Journal of Criminal Justice*, vol. 23, no. 1, pp. 13-27.

Dobson, C. & Payne, R. 1982, *The Terrorists: Their Weapons, Leaders and Tactics*, revised edn, Facts on File, New York.

Grabosky, P. N. 1998, *Technology and Crime Control*, Trends and Issues in Crime and Criminal Justice, No. 80, Australian Institute of Criminology, Canberra.

Grabosky, P. N. & Smith, R. G. 1998, *Crime in the Digital Age: Controlling Telecommunications and Cyberspace Illegalities*, Federation Press, Sydney;Transaction Publishers, New Brunswick, NJ.

Harding, R. W. 1983, "An ounce of prevention . . . Gun control and public health in Australia", *Australian and New Zealand Journal of Criminology*, vol. 16, pp. 3-19.

Hewitt, J. 1996, *Ancient Armour and Weapons*, Bracken Books, London.

Jayasuriya, D. C. 1998, "The role of chemicals control in the fight against illicit drug production and trafficking", *Journal of Financial Crime*, vol. 5, no. 3, pp. 272-5.

Johnson, L. C. 1997, "The fall of terrorism", *Security Management*, vol. 41, no. 4, pp. 26-32.

Leader, S. H. 1997, "The rise of terrorism", *Security Management*, vol. 41, no. 4, pp. 34-9.

Lewis, A. 1997, "Toxic gases: The terrorists' next weapon", *International Journal of Risk, Security and Crime Prevention*, vol. 2, no. 4, pp. 315-17.

Morello, C. 1996, "Computers forbidden fruit for paroled hacker", *Salt Lake Tribune*, 15 September, http://www.sltrib.com/96/SEP/15/twr/01254824.htm.

Mukherjee, S., Carcach, C. & Higgins, K. 1997, *A Statistical Profile of Crime in Australia*, Research and Public Policy Series No. 7, Australian Institute of Criminology, Canberra.

Office of Strategic Crime Assessments and Victoria Police 1997, *Computer Crime and Security Survey*, Office of Strategic Crime Assessments and Victoria Police.

Smith, R. G. 1997, "Medicine, crime and unprofessional conduct in the on-line world", *Medico-Legal Journal*, vol. 65 , no. 3, pp. 133-8.

Victoria Police 1997, *Crime Statistics 1996-97*, Victoria Police, Statistical Services Division, Melbourne.

Dr Russell G. Smith is a Research Analyst with the Australian Institute of Criminology

General Editor, Trends and Issues in Crime and Criminal Justice series:
Dr Adam Graycar, Director
Australian Institute of Criminology
GPO Box 2944
Canberra ACT 2601 Australia

Note: Trends and Issues in Crime and Criminal Justice are refereed papers.