The challenge of the forensic investigation of computer crime

By Commander Barbara Etter, Director, Australasian Centre For Policing Research

In an address to the Australian Institute of Criminology's 4th National Outlook Symposium on Crime in Australia which took as its theme: *New Crimes or New Responses*, held in Canberra during June 21-22 this year, Commander Babara Etter outlined current e-crime trends and speculated as to the challenges that law enforcement agencies will have in coping with e-crime in the future.

Commander Barbara Etter

E-crime[1] presents as one of the major challenges of the future to Australasian law enforcement. As Information and Communications Technology (ICT) becomes even more pervasive and aspects of electronic crime feature in all forms of criminal behaviour, even those matters currently regarded as 'traditional' offences.

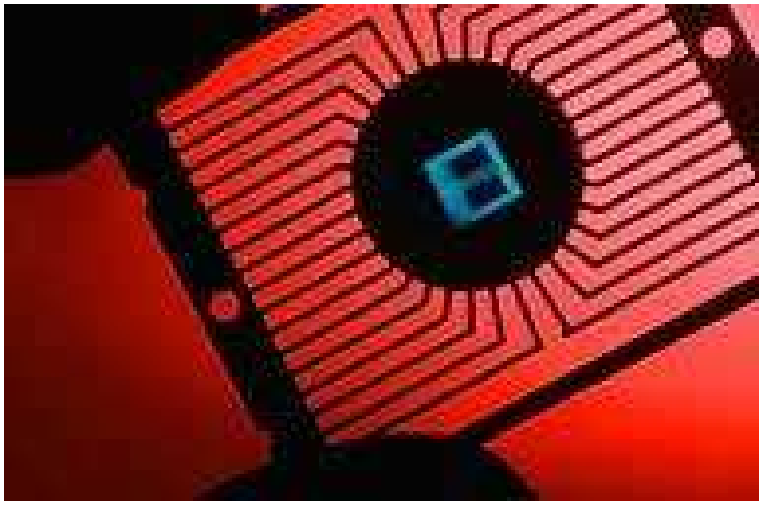
ICT will also feature in many transnational crimes involving drug trafficking, people smuggling and money laundering and while many e-crimes will be 'old style' crimes simply involving the use of ICT, new forms of crime will also emerge. In addition, the barriers to committing crime, that is electronic crime, have dropped significantly and criminals are becoming even younger. It would seem that people who would not dream of stealing or maliciously damaging other people's property in real life have no qualms or second thoughts in relation to the opportunities and challenges presented by the Internet.

In some respects, the growth in the uptake of ICT, including the Internet, presents as great a challenge for policing as the introduction of the telephone and the motor vehicle. Some argue that it is merely a case of the 'same old wine in new bottles'. This paper argues that, while there will always be a role for traditional investigative techniques, e-crime presents as a new form of business that will require a fundamental paradigm shift in policing. Dealing with the global aspects of the issue will be particularly challenging.

Policing will also need to be very selective about the range of e-crime incidents that it responds to and must carefully determine assessment and prioritisation models, as there will never be complete policing of all e-crimes. Moreover, the costs of investigation will be high and there will be a need to respond in a much shorter time frame, increasing pressure on already stretched resources.

This article attempts to:

- discuss the nature of the e-crime or computer crime



problem and the challenges it presents;
- identify and discuss the new response issues which may be encountered during the prevention, detection and investigation of e-crime; and
- outline what Australasian policing is doing to prevent and reduce the incidence of this type of crime.

The environment

As most of us are aware, Australia has been avid in its uptake of technology and is among the leading nations in terms of key measures of Internet infrastructure, penetration and activity (NOIE 2000a, p.4). The most recent National Office for the Information Economy (NOIE 2000b) report entitled *The Current State of Play* provides the following points of interest:

- In the year to May 2000, an estimated 46 per cent of adult Australians accessed the Internet (NOIE 2000b, p.8).
- In the year to May 2000, an estimated 33 per cent of Australian households had home Internet access (an increase of 135 per cent since May 1998) (NOIE 2000b, p.8).
- 802,000 Australian adults (or 6 per cent of all Australian adults) shopped via the Internet in the 12 months to May 2000, an increase of around 152,000 adults during the year preceding May 1999 (NOIE 2000b, p.5).
- Internet banking and online bill payment increased 810 per cent between May 1998 and May 2000 (NOIE 2000b, p.6).

This rapid increase in the use of computer technology has facilitated Australia's participation in the emerging Information Economy, but also increases its exposure to electronic crime issues.

Technology, particularly ICT, is becoming more and more pervasive in our society. The use of the Internet will continue to evolve and grow in many areas including (California High Technology Crime Advisory Committee (CHTCAC) 2000, p.26):

- Electronic commerce;
- Online banking;
- Drug stores with prescription services;
- Health care services and records; and
- Education.

Of particular relevance to those interested in crime issues is the potential for huge increases in fraud. Fraud (including forgery and false pretences) has already been found to be the most expensive crime in Australia, costing the Australian community in monetary terms up to $3-$3.5 billion per year or 15.3-17.9 per cent of total crime costs (Walker 1997, p.6). The enormous potential for growth in this area was recognised by the Australasian Police Ministers' Council (APMC) at its meeting in Perth on July 12, 2000. As a result, a national project is being undertaken to examine the possibility of developing an approach to ensure that fraud is addressed in a systematic, coordinated and standardised way. The APMC recognised that the possibilities for misuse of electronic technologies made this an issue which needed to be addressed immediately.

Identity theft, in particular, which can facilitate a range of fraud offences, seems to be a growing concern. As the Office of Strategic Crime Assessments (OSCA) stated in a recent report on the changing nature of fraud in Australia (2000, p.10):

Technology has weakened the integrity of many identifiers currently in use — birth certificates can be reproduced using desktop publishing software; counterfeit passports and counterfeit smartcards can be purchased over the Internet. Easier access to these false identifiers facilitates a range of fraudulent behaviour, including tax evasion, immigration malpractice, fraudulent claims against social security and health insurance companies. It also assists in hiding the proceeds of frauds.

Consider for a moment that a website operated by Harvey Norman reportedly had to be shut down because a quarter of the orders placed on it were on stolen credit cards (The Advertiser, 30 August 2000, p.13). In addition, a recent study found that 12 times more credit card fraud occurred on Internet transactions than on conventional sales (The Advertiser, 30 August 2000, p.13). Another global report emanating from the UK found that e-commerce firms were reporting up to 25 per cent of online transactions as fraudulent, with an average of 5 per cent. Stolen credit cards and identity theft made up the majority of frauds perpetrated on the Internet - 28 per cent and 20 per cent respectively (Wakefield 1999).

The computer has become an integral part of our way of life. However, as our dependency on ICT increases, so too does our vulnerability. This vulnerability and associated implications for investigators was clearly demonstrated in recent times with:

- The distributed denial of service attacks on Yahoo, eBay and other major Internet players;
- The security breach in Australia involving the ABN/GST website (Van Dijk 2000);
- The 'Love Bug' virus (or ILOVEYOU worm);
- The reported denial of service attacks on the St George Bank in September (Kaye 2000, p.1; Spencer and O'Brien 2000, p.29);
- The recent hacking of Microsoft where an attacker apparently gained access to the source code for a future product (Gliddon 2000; Weiss 2000);
- The large scale theft of more than one million credit card details from various US e-commerce sites by Russian and Ukrainian crime gangs (Hellaby 2001);
- Attacks on government websites in the US, UK and

Australia by Pentaguard in January 2001, said to be one of the largest most systematic defacements of worldwide government servers on the www (Legard 2001); and

- The largest identity theft case in Internet history involving 200 of the 400 richest people in America listed in Forbes magazine, which was recently discovered in the US (Weiss 2001).

Some of these incidents also demonstrate the capacity for a single individual to perpetrate major and widespread criminal harm (with a 12-year-old Canadian boy, named 'Mafia Boy', an alleged offender in the denial of service attacks, a New York bus boy allegedly responsible for the large scale ID theft scam and a university student from the Philippines the apparent offender in the Love Bug incident). The ABN/GST incident (described below) was also referred to as involving a 'novice' and as 'very unsophisticated hacking, requiring little skill' (Van Dijk 2000, pp.1 & 4).

One can only wonder about the extent of damage that could occur in the case of highly-skilled, well-orchestrated and maliciously motivated attacks. For instance, one hacker collective, Lopht, gave evidence to a US congressional investigation that it could halt all Internet activity within 30 minutes (James and Cooper 2000).

As indicated in the introduction, the barriers to participating in criminal activity appear to be dropping and there is also a proliferation of individuals who are capable of countering IT security measures. For instance, it was believed a few years ago that only several thousand people in the US had the capabilities to launch a cyber-attack. Today, it is estimated that there are 17 million such people in the US alone (O'Brien and Nusbaum 2000).

The 2000 GST/ABN incident

A student known variously as K2 and Kelly exposed a glaring security breach in the Australian GSTAssist website. Simply by typing in a string of numbers, K2 was able to access the records of more than 20,000 GST-registered providers, including their bank details. He alerted more than 17,000 of the providers by emailing their confidential details to them. K2 rejected the notion he was a hacker, saying it involved no cracking, but was a wide open security flaw (Dancer 2000, p.76).

Forbes' 400 Richest People ID Theft Case

Using computers in a local library, a Brooklyn busboy pulled off the largest ID theft in Internet history, victimising more than 200 of the richest people in America listed in Forbes' magazine. He cunningly used the web to invade the personal financial lives of celebrities, millionaires and corporate executives. Abdullah, 32, a pudgy convicted swindler and high school dropout, is suspected of stealing millions of dollars. He allegedly breached the bank, brokerage and credit card accounts of people such as Steven Spielberg, George Lucas, Oprah Winfrey, Ross Perot etc.

Abdullah duped companies into providing credit reports on his victims. He then used the confidential data to clone their IDs and gain access to their credit cards and accounts at some of the most prestigious brokerage houses and investment banks. For more than six months, Abdullah allegedly worked his scam, remaining nothing more than an electronic pulse on the web. He was recently charged with possession of forged devices, stolen property and criminal impersonation.

After his arrest, police recovered a dog-eared copy of Forbes' 400 richest people in America. On page after page, next to biographies and photos of the rich and famous were addresses, cell phone and social security numbers, bank and brokerage account numbers and balances - even mothers' maiden names, all meticulously jotted down (Weiss 2001).

The nature of the e-crime problem

Global connectivity means that havoc can occur, in a very short timeframe, throughout the world. The abuse of computer technology may threaten national security, public safety and community well-being, and devastate the lives of affected individuals.

A long list of traditional offending has been greatly facilitated by technology advancements such as mobile telephony, the Internet and encryption (President's Working Group on Unlawful Conduct on the Internet (PWGUCI) 2000, p.1).

Furthermore, new criminal opportunities or new crimes have been created by the development of

electronic media. Denial of service attacks, viruses, unauthorised entry, information tampering, cyberstalking, spamming, page-jacking, dumping or phone-napping, and computer damage are relatively new types of offending or undesirable behaviour that did not exist in the pre-computing environment. Likewise, the development of computers has created new opportunities for services theft, manipulation of the stockmarket (through ramping up of stock prices and 'pump and dump' schemes using the Internet), software piracy, and other thefts of intellectual property.

Because many telecommunications networks, such as the public telephone network and the Internet, are now connected globally, there is an international dimension often added to the offending. It has been suggested that with modern mobile devices such as laptop computers, mobile phones and modems, crimes can also now be committed anytime anywhere, with the potential scale of the crime scene and the impact of the offending potentially the entire network-connected world (Bliss and Harfield 1998).

Electronic crime is variable in its manifestations, so it is difficult to discuss in terms of aggregate incidence and impact. This inability to accurately define the nature of the problem is not helped by the fact that currently no statistics on computer crime are maintained by Australasian police. Unfortunately, definitive information on the present extent and impact of electronic crime both in Australia and overseas is not available. A significant amount of this crime is simply not reported and some may not even be detected. This non-reporting is in part because of a great reluctance to notify incidents to law enforcement authorities so as to avoid any potentially adverse impact on consumer confidence or share prices, or perhaps because of a lack of confidence in law enforcement to deal with such issues in a timely or effective way.

Two major surveys on computer crime have been conducted in recent years in Australia: one in 1997 by OSCA and Victoria Police, the other in 1999 by Deloitte Touche Tohmatsu and the Victoria Police.

The 1997 survey claimed that Australian industry was 'under threat'. A representative sample of over 300 Australian companies was surveyed. Of the respondents, 37 per cent had experienced some form of intrusion or unauthorised use of computer systems in the past 12 months. Nearly 90 per cent of companies that had experienced computer-related incidents had been subjected to attacks from sources internal to their own organisation. More than 60 per cent were subjected to intrusions from external sources (meaning that a significant number of companies had been subjected to attacks from both employees and outsiders).

Issues highlighted by the survey (OSCA and Victoria Police 1997) included:

- Australian industry was subject to a significant level of computer security incidents at a rate comparable to the US;
- the threat from outsiders appeared to be growing;
- a primary target of attacks was Australia's banking and finance industry, which was also a critical component of the National Information Infrastructure (NII); and
- there appeared to be a direct correlation between increasing dependence on sophisticated IT and a growing level of vulnerability to attack.

The 1999 Computer Crime and Security Survey was sent to the 350 largest Australian companies in November 1998. The key findings included (Deloitte Touche Tohmatsu and Victoria Police 1999):

- one third of the companies surveyed reported an attack in the past 12 months;
- 83 per cent of those companies that reported being aware of an intrusion had been attacked from an internal source and 58 per cent had been attacked from an external source;
- of those companies that were attacked, 42 per cent did not report the incident outside the company;
- attacks against organisations appeared to be random and opportunistic, in that only 12 per cent of those attacked suffered losses in excess of $10,000;
- according to respondents, the most likely motivation for an attack was curiosity (71 per cent); and
- the attacker was most likely to be a disgruntled employee or an independent hacker.

In the 1999 survey, companies were concerned that attacks would become more organised and premeditated. Havking remained the greatest concern for the future (at 64 per cent).

Indications are that electronic crimes are more than likely on the increase. For instance, AusCERT (the Australian Computer Emergency Response Team), Australia's peak agency assisting in the prevention of computer-based attacks, has confirmed that Australia has seen a dramatic rise in the number of reported cyber incidents.

In 2000, a total of 8197 computer security incidents were reported to AusCERT, representing a four-fold increase on the number reported in 1999 (University of Queensland 2001). Such incidents were commonly either network scans, viruses or distributed denial of service attacks. The statistics provided by AusCERT for the past three years are of concern as they demonstrate an alarming increase in such incidents:

1998 . . . . . *1342*
1999 . . . . . *1816*
2000 . . . . . *8197*

The US 2001 Computer Crime and Security

Survey (CSI 2001) also indicated some alarming increases and trends. The survey found that the threat from computer crime continues unabated and that the financial toll is mounting. It also found increases in the reported incidence of detected system penetration from the outside, denial of service attacks and computer viruses. There was an increase in reported financial losses with 186 respondents in the most recent survey reporting losses in the order of $US378 million compared to losses reported by 249 respondents in 2000 of $US266 million.

The editorial director with the CSI is reported as saying (Hatcher 2001):

"The stereotypical hacker is a juvenile with a blue Mohawk and skateboard and is a genius. … They are not where these numbers come from."

This comment is of concern as it would appear that activity is becoming more organised and professional. Consider too that it has been reported that the Chinese triads have been employing computer programmers since 1998 (Galeotti 2000). In addition, the Aum Shinriko sect, which was responsible for the deadly sarin nerve gas attack in a Tokyo subway in 1995, has diversified into the IT industry. The sect reportedly was responsible for the installation of more than 100 computer systems into Japanese government ministries and major companies, thus raising fears over how the Aum could exploit its cyberwarfare potential through its access to government computers (O'Ballance 2001).

In summary, we are clearly witnessing exponential growth in the uptake of technology and the use of the Internet. It is reasonable to assume that such growth will be accompanied by an increase in the incidence of electronic crime. There have been predictions that online crime will grow by as much as 1000 per cent over the next four years (Agence France-Presse (AFP) 2000). At this point in time, it is difficult to know what is occurring in this area due to a clear reluctance by industry and others to report many electronic crimes to police. Part of the response to this issue will be measures to enhance our understanding of the nature of the problem.

Unique challenges and related response issues

While computer technology will continue to be used in many traditional crimes, the nature and particular features of electronic crime, will pose new and unique challenges for investigators such as.

- offender anonymity;
- global reach (including issues of jurisdiction, disparate criminal laws and the potential for large scale victimisation);
- the speed at which crimes can be committed;
- the potential for deliberate exploitation of sovereignty issues and cross-jurisdictional differences by criminals and organised crime;
- the volatility or transient nature of evidence, including no collateral or forensic evidence such as eyewitnesses, fingerprints or DNA; and
- the high cost of investigations.

As indicated above, the potential for huge increases in fraud is very real. There is also the potential for organised crime to exploit the gaps in the current law enforcement and revenue protection response in order to conduct their illegal business and to successfully launder the proceeds of crime. It has been estimated that US$500 billion is laundered globally each year (CHTCAC 2000, p.32).

Computer technology also provides an effective tool for terrorists and foreign intelligence organisations. As James and Cooper stated (2000, p.53):

> The Internet provides activists, from the protester to the hardened terrorist, with the means to apply a full range of tactics, including protest and blockade, disruption and destruction, potentially leading to the loss of life. The 'cyber option' not only enhances the traditional roles and traits of terrorism, but also offers new forms of attack and a range of targets hitherto unavailable.

The challenges of the digital age and for the management of serious crime are numerous and diverse, and include (Police Commissioners' Conference Electronic Crime Working Party 2000, pp. 25-28; Rees 2000, pp.16-19):

- bridging multijurisdictional boundaries;
- retaining and preserving evidence;
- acquiring appropriate powers;
- decoding encryption;
- proving identity;

- knowing where to look for evidence;
- tackling the tools of crime and developing tools to counter crime;
- rethinking the costs and priorities of investigation;
- responding to crime in real time;
- coordinating investigative activities;
- Improving training at all levels of the organisation;
- developing strategic partnerships and alliances;
- improving the reporting of electronic crime;
- enhancing the exchange of information and intelligence;
- acquiring, developing and retaining specialist staff; and
- avoiding 'tech-lag' (or ensuring access to cutting edge technology).

One of the biggest policy issues for government will be how to deal with the anonymity of the Internet. Indeed, the US Electronic Frontier report (PWGUCI 2000) states that 'balancing the need for accountability with the need for anonymity may be one of the greatest policy challenges in the years ahead'.

The UK has also demonstrated its concern relating to anonymity and a range of other issues through the creation of the Regulatory and Investigatory Powers Act (RIPA) which, after much controversy, received royal assent in July 2000.

The FBI's Carnivore system has also been the subject of much criticism and debate. In Australia, dealing with the anonymity issue will involve, inter alia, developing new response capabilities in close cooperation with Internet Service Providers (ISP's).

Australasian Commissioners of Police, recognising the complexity and immediacy of this issue, formed a Steering Committee comprised of four Commissioners of Police, and a Working Party, chaired by the Director of the ACPR, at their March 2000 Commissioners' Conference, the theme of which was *Crime @the speed of thought.*

The major task of the Working Party was to prepare a draft Australasian law enforcement strategy on electronic crime and a related task was to evaluate the current law enforcement response capacity.

The Working Party was also requested, as a first step, to scope out the nature of the electronic crime problem. In September 2000, the Working Party finalised and published a comprehensive and detailed report entitled 'The Virtual Horizon: Meeting the Law Enforcement Challenges' (Police Commissioners' Conference Electronic Crime Working Party 2000).

The scoping paper, inter alia, examines a number of capability issues such as:

- training and education;
- forensic computing capability;
- skills acquisition, development and retention; and
- information and intelligence exchange.

The Working Party also examined the legislative environment in a national/Australasian and international context in relation to substantive criminal law and procedural issues relating to the investigation of computer crime.

In addition to substantive criminal offence provisions, the Working Party identified some key procedural issues consistent with the findings of the 1998 National Police Research Unit (NPRU) report on minimum legislative provisions for computer crime (Thompson and Berwick), which had been strongly endorsed by the APMC in 1997. Issues identified as requiring further and urgent attention in the scoping paper include:

- computer search and seizure (including computer network and extra-territorial searches);
- undercover computer investigations (including covert data collection and immunity from prosecution issues);
- obligations of system owners (including the ability to get around encryption);
- computer communications interception and monitoring (including data communications interception and call tracing and network monitoring); and
- data retention and preservation.

A major issue which also needs to be dealt with, and which was discussed by the Model Criminal Code Officers Committee (MCCOC 2000 and 2001), is the issue of jurisdiction. This matter is particularly problematic given the potential global reach or borderless nature of electronic crime. For instance, it would be particularly easy to thwart a criminal investigation or prosecution at the present time by routing your transactions through a number of countries (particularly those with weaker law enforcement regimes or those without relevant treaty arrangements). We are also seeing the emergence of data havens, such as the Principality of Sealand, an island fortress 10 km off the English coast, where anyone who wants to keep a website or other data out of the reach of national governments can rent space on the Sealand servers (The Economist 2001).

As the United Nations (UN) points out (1999, p.48):

> Today, it is technologically possible for an operator to punch a keyboard in country A so as to modify data stored in country B, even [though] the operator does not know that the data are stored there, to have the modified data transferred over a telecommunications network through several other countries, and to cause an outcome in country C. On the basis of the physical act, three or perhaps more countries will

have been involved and may have a claim to jurisdictional competency.

Depending on which elements or stages of the crime are given priority, several countries in the above scenario could, within their full sovereignty, declare the incident as having occurred on their territory, thus invoking the principle of territorial jurisdiction in order to prosecute and sanction. This raises a potential jurisdictional conflict, as well as the question of the appropriate arbitration of these equal claims for jurisdiction (UN 1999, p.48).

Jurisdiction presents as a very real issue in the area of electronic crime and will require new responses from law enforcement particularly when one considers the need for a much more rapid response.

In the international context, some of the key problems in the area of computer crime have been identified (UN 1999, p.3) as:

- the lack of global consensus on what types of conduct should constitute a computer-related crime;
- the lack of global consensus on the legal definition of criminal conduct;
- the lack of expertise on the part of police, prosecutors and the courts in this field;
- the inadequacy of legal powers for investigation and access to computer systems, including the inapplicability of seizure powers to intangibles such as computerised data;
- the lack of harmonisation between the different national procedural laws concerning the investigation of computer-related crimes;
- The transnational character of many computer crimes;
- the lack of extradition and mutual assistance treaties and of synchronised law enforcement mechanisms that would permit international cooperation, or the inability of existing treaties to take into account the dynamics and special requirements of computer crime investigation.

To date, international harmonisation of the legal categories and definitions of computer crime has been proposed by the UN, Organisation for Economic Cooperation and Development (OECD) and the Council of Europe (UN 1999, p.22). However, before we even contemplate harmonisation, it will be necessary to get many (if not all) countries to agree to legislate in this area. One US survey found that of 52 nations surveyed, 33 did not even have laws which dealt with computer crime (AFP 2000).

The Council of Europe's draft Convention on Cybercrime (COE 2000) illustrates some of the difficulties of dealing with the issue of electronic crime in a global sense and the need for new types of responses.

The Convention aims principally at:

- harmonising the domestic criminal substantive law elements of offences and connected provisions in the area of cybercrime;
- providing for domestic criminal procedural law powers necessary for the investigation and prosecution of such offences as well as other offences committed by means of a computer system; and
- setting up a fast and effective regime of international cooperation.

In relation to international cooperation, the draft treaty requires future parties to provide each other with various forms of assistance, including the preservation of evidence and the locating of online suspects. The document also deals with certain aspects of transborder computer searches. Traditional forms of mutual assistance and extradition are available under the draft Convention and a round-the-clock network of national contact points is proposed to accelerate international investigations. The text of the draft Convention may be found on: http://conventions.coe.int/treaty/EN/projects/cybercrime.htm.

It is clear that the transborder search of data banks is problematic (UN 1999, p.50; UNAFEI 2000). Criminal investigators will increasingly be faced with the problem of how to retrieve data, as potential evidence, that are stored abroad, when investigating by means of online access to those data (UN 1999, p.51). The question is whether the investigator may penetrate the database by direct access, without the intervention, knowledge or agreement of the State in which the data are located (UN 1999, p.51). The UN states (1999, p.51) that the view that the deliberate investigation of online data constitutes a violation of the sovereignty of the other State is probably correct.

Mutual assistance is another area which may be problematic in relation to electronic crime. The matter is currently being examined by the Action

Group into the law enforcement implications of Electronic Commerce (AGEC), chaired by Ms Elizabeth Montano, the Director of AUSTRAC.

The general proposition is that, if a country requires assistance from another country which involves the exercise of compulsory powers in that country, the matter must be processed by way of a formal Mutual Assistance (MA) request. The main types of assistance provided relate to:

- the execution of search warrants and notices to produce;
- taking evidence; and
- restraining and recovering the proceeds of crime.

One of the most common complaints about MA is the time that it takes to process an MA request. It appears that in the best of circumstances it is still unusual to get a response to an MA request in less than two to three months. Therefore, this regime cannot be used to provide assistance on a real-time or close to real-time basis.

It is evident that the legislative issue is a critical one and ongoing and significant regulatory and legislative reform to enable new types of responses at the jurisdictional, national and international levels will be required to effectively address electronic crime issues.

New responses require new skills and knowledge. In relation to training, much more needs to be done to ensure that all law enforcement personnel have a basic understanding of search and seizure issues in relation to electronic evidence, for instance. There is also a need for more advanced and ongoing training for those involved in the investigation of electronic crime and for specialist training for a cadre of expert staff involved in the forensic computing area.

Skills acquisition, particularly in the form of specialist forensic computing staff, will be increasingly difficult as we compete with the private sector and the market dictates high prices for such expertise. The 'brain drain' issue will continue to present a significant challenge for policing as our experts are lured elsewhere. New responses will also be required to deal with the issue of accessing appropriate expertise, which will come at a high cost indeed. This may well involve the greater use of outsourcing to the private sector.

A related issue which is examined in the Police E-crime Working Party's scoping paper is the current state of police forensic computing capabilities, as well as the need for a national capability.

It is also apparent that much more needs to be done to facilitate the exchange of information and intelligence between policing and the community, as well as the private sector, in order to detect, prevent and respond to electronic crime. Initiatives of the National Infrastructure Protection Center in the United States, such as Outreach and InfraGard, are instructive in this regard (NIPC n.d.). So too are recent developments in the US in relation to the formation of various ISAC's or Information Sharing and Analysis Centers.

It was reported recently that a group of 19 technology vendors in the United States announced the formation of an alliance that is supposed to provide a conduit for sharing information about viruses and other potential threats to corporate and government computer networks (Verton 2001). Plans for the IT Information Sharing and Analysis Center (IT-ISAC) were detailed by government officials and participants such as Cisco Systems, Computer Sciences, IBM, Hewlett-Packard, Microsoft, and Oracle. Their goal is to set up a secure mechanism that companies can use to exchange information about security vulnerabilities with each other and government agencies. The new virtual data-sharing centre will be oversighted by a Board of Directors drawn from many of the founding members. The formation of the IT-ISAC was described as 'a giant step forward' in the protection of the nation's information networks.

Fighting electronic crime will be an expensive endeavour and there are clear benefits in the strategic sharing of scarce resources. It may even be necessary to consider the development of a national centre for cybercrime to strategically assess, prioritise and task agencies in relation to e-crime matters. This may involve a joint venture with the private sector, as has occurred with the NIPC in the US.

The lack of such a facility may limit our international response capability and could lead to unnecessary duplication of effort or the compromise of the integrity of an investigation. It also means that there would be little capacity to detect low value/high volume fraud, organised crime and international scams.

Australasian Police Commissioners are moving to address a wide range of prevention and response issues through the implementation of their E-crime Strategy, the development of which arose from resolutions of the 2000 Police Commissioners' Conference.

The Police Commissioners' Conference E-crime Strategy

Following on from the scoping exercise, an analysis was undertaken by the Working Party and a strategy developed. The strategy was launched by Commissioners at the International Policing Conference held in Adelaide in early March 2001. Copies of the document are available from both the ACPR and AFP websites www.acpr.gov.au and www.afp.gov.au.

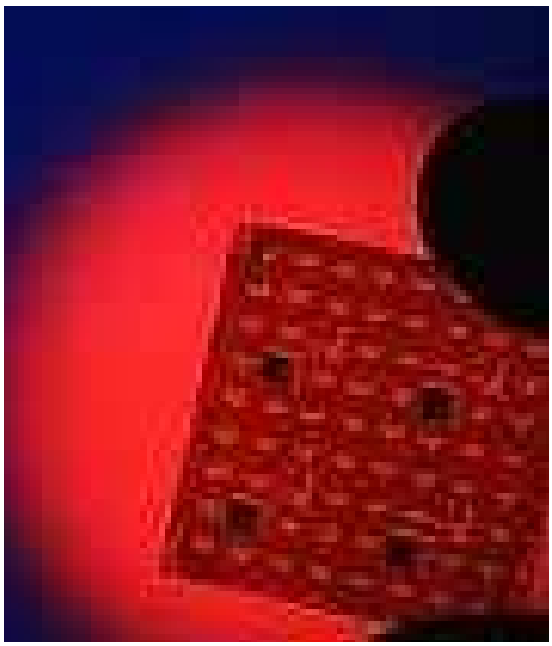
At this stage, the strategy identifies 5 important

focus areas which are inextricably linked and will have limited impact unless dealt with collectively. They are:

- prevention;
- partnerships;
- education and capability;
- resources and capacity; and
- regulation and legislation.

Complementary workplans which address each of these focus areas have also been developed and action will be taken to implement priority taskings, as resources allow. Every effort will be made to ensure that the strategy leverages off a variety of initiatives already in place.

Strategic and effective partnerships with the community and the private sector will be absolutely essential to success. Such partnerships must be genuine, mutual and cooperative. A major thrust of the strategy is also prevention which will involve a whole of government approach to a range of issues. For instance, community education and the development of cyberethics will also be important in responding to the issue and raising the barriers to crime.



One of the major challenges in developing new responses will be successfully engaging the private sector. Clearly, it will be necessary to persuade CEO's and other business leaders that the issue of on-line security and e-crime is a matter of good corporate governance which needs to be integrated throughout any business strategy. Unfortunately, it would seem that too many corporate leaders currently regard the matter as a technical issue to be dealt with by IT departments. A 'wake-up call' even more significant than the Love Bug may unfortunately be required to galvanise activity.

The use of joint taskforces involving the private sector and the establishment of essential infrastructure as joint ventures (as has occurred with the NIPC in the United States) may need to be further explored. Such partnerships may become quite common features of response mechanisms and investigations in the future.

The Police Commissioners' Conference Strategy will position police to enable an effective response to a wide range of local and global crimes which utilise or target the Internet and ICT. However, it must be kept in mind that we are not just talking about esoteric IT-specific crimes when seeking to establish a prevention and response capacity in this area. It is recognised that computers will increasingly feature in the crime scenes of many 'traditional' crimes and that new skills, approaches and technologies are required to simply maintain current levels of effectiveness. Police must be as adept at dealing with a crime scene featuring a computer or related technology as they are currently with crime scenes without technological dimensions.

Conclusion

It is true that many e-crimes of the future will be traditional crimes simply perpetrated via or facilitated through the use of ICT. However, as indicated above, there are characteristics of electronic crime, such as anonymity, speed, the ease with which one can participate in unlawful behaviour and the potential for large scale victimisation, that will present new and unique challenges. The ability to move quickly to preserve data and to get around encryption will also require new responses.

E-crime is truly a global issue and there will be an unprecedented need for international coordination and cooperation. An example of innovative responses in this area is a recently announced initiative in relation to dealing with cross-border Internet fraud and improving consumer confidence in e-commerce. A multilingual website www.econsumer.gov will provide information on consumer protection laws in 13 countries and offer consumers a way to file complaints online. The cooperating governments will use a parallel, but secure, site to share complaint data and information on e-commerce fraud investigations. The 13 countries are: Australia (through participation of the Australian Competition and Consumer Commission (ACCC)), Canada, Denmark, Finland, Hungary, Mexico, New Zealand, Norway, South Korea, Sweden, Switzerland, the UK and the US. The plan is said to be backed by the OECD.

A response to electronic crime will involve much stronger partnerships with the private sector and other law enforcement and related agencies (such as defence and intelligence) and a major thrust of

addressing the issue must be one of prevention, otherwise policing will simply be overwhelmed. It will also be important to understand the nature of the problem and to address the significant under-reporting of the phenomenon.

Policing also needs to market the clear message that there will never be full policing of all e-crimes. The role of policing in response to various computer crime incidents will need to be articulated. In addition, assessment and prioritisation models will need to be carefully determined and communicated to relevant stakeholders.

New skills, technologies and investigative techniques will be required to detect, prevent and respond to electronic crime. This is not just about a realignment of existing effort. This 'new business' will be characterised by new forms of crime, a far broader scope and scale of offending and victimisation, and challenging technical and legal complexities. Innovative responses such as the creation of 'cybercops', 'cybercourts' and 'cyberjudges' may eventually be required to overcome the significant jurisdictional issues.

It is clear that much more needs to be done to enhance our capacity to respond to incidents of computer crime, both nationally and internationally. Managing the response to and the investigation of such crime will indeed be complex and challenging. The Police Commissioners' Conference E-crime Strategy provides a valuable framework and set of guiding principles to fashion a range of new responses.

References

Agence France-Presse (AFP) 2000, 'Much international Internet crime goes unpunished: net crime study', http://www.it.fairfax.com.au/breaking/20001208/A62215-2000Dec8.html, visited 12 November 2000.

Bliss, A. & Harfield, C. 1998, 'The threat of computer crime: identifying the problem and formulating a response at force level', *The Police Journal*, January, Butterworths, Surrey, UK, pp.25-34.

California High Technology Crime Advisory Committee (CHTCAC) 2000, *Annual Report on High Technology Crime in California*, California High Technology Crime Advisory Committee, Sacramento, CA, http://www.ocjp.ca.gov/pub_CHTCAC_annu1.pdf, visited 31 March 2000.

Computer Security Institute 2001, 'Financial losses due to Internet intrusions, trade secret theft and other cyber crimes soar', http://www.gocsi.com/prelea_000321.htm, visited 16 March 2001.

Council of Europe (COE) 2000, *European Committee on Crime Problems (CDPC) Committee of Experts on Crime in Cyberspace (PC-CY) Draft Convention on Cybercrime (Draft No. 24 Rev.2)*, http://conventions.coe.int/treaty/EN/cadreprojets.htm, visited 16 February 2001.

Dancer, H. 2000, 'K2 uncovers GST keyhole', *The Bulletin*, 11 July, p.76.

Deloitte Touche Tohmatsu & Victoria Police 1999, *Computer Crime & Security Survey*, Deloitte Touche Tohmatsu & Victoria Police, Melbourne.

Galeotti, M. 2000, 'Chinese crime's global reach', *Jane's Intelligence Review*, November, pp.10-11.

Gliddon, J. 2000, 'Cracks in the armour', *The Bulletin*, 7 November, p.86.

Hatcher, T. 2001, 'Costs of computer security breaches soar', 12 March, http://www.cnn.com/2001/TECH/internet/03/12/csi.fbi.hacking.report/index.html, visited 21 March 2001.

Hellaby, D. 2001, 'Warning over credit card sting', *The Australian*, IT section, 20 March, p.32.

James, L. & Cooper, J. 2000, 'Organised exploitation of the information super-highway', *Jane's Intelligence Review*, July, pp.52-55.

Kaye, B. 2000, 'St George still a 'sitting duck'', *Computerworld*, Vol.24 No.11, 11 September, pp.1 & 4.

Legard, D. 2001, 'Hackers hit government sites', *Computerworld*, Vol.24 No.26, 29 January, p.12.

Model Criminal Code Officers Committee (MCCOC) 2000, 'Chapter 4: Damage and computer offences', *Model Criminal Code*, January.

Model Criminal Code Officers Committee (MCCOC) 2001, 'Chapter 4: Damage and computer offences and amendment to Chapter 2: Jurisdiction', Model Criminal Code, Report, January.

National Infrastructure Protection Center (n.d.), 'Outreach/Infragard', http://www.fbi.gov/nipc/outreachinfragd.htm, visited 25 May 2000.

National Office for the Information Economy (NOIE) 2000a, *The Current State of Play- July 2000*, NOIE, Canberra, http://www.noie.gov.au/information_economy/ecommerce_analysis/ie_ stats/StateOfPlay/index.htm, visited 24 August 2000.

National Office for the Information Economy (NOIE) 2000b, The Current State of Play - November 2000, NOIE, Canberra, http://www.noie.gov.au/projects/information_economy/ecommerce_analysis/ie_ stats/StateofPlayNov2000/index.htm, visited 13 February 2001.

O'Ballance, E. 2001,'From Sarin to Cyber Warfare: The Aum Doomsday Sect', *Intersec*, Vol.11 Issue 2, February, pp.52-53.

O'Brien, K. & Nusbaum, J. 2000, 'Intelligence collection for asymmetric threats - Part Two', *Jane's Intelligence Review*, November, pp.50-55.

Office of Strategic Crime Assessments (OSCA) & Victoria Police 1997, *Computer Crime and Security Survey*, OSCA / Victoria Police, Melbourne.

Office of Strategic Crime Assessments (OSCA) 2000, 'The Changing Nature of Fraud in Australia', Attorney-General's Department.

Police Commissioners' Conference Electronic Crime Working Party 2000, *The Virtual Horizon: Meeting the Law Enforcement Challenges. Developing an Australasian law enforcement strategy for dealing with electronic crime. Scoping Paper*, Australasian Centre for Policing Research, Report Series No: 134.1, Adelaide.

President's Working Group on Unlawful Conduct on the Internet (PWGUCI) 2000, *The Electronic Frontier: The Challenge of Unlawful Conduct Involving the Use of the Internet,* PWGUCI, Washington, DC, http://www.usdoj.gov/criminal/cybercrime/unlawful.htm, visited 9 March 2000.

Rees, Andrew 2000, *ACPR Technology Environment Scan*, Report Series No: 133.1, Australasian Centre for Policing Research, Adelaide.

Spencer, S. & O'Brien, S. 2000, 'Internet banking service attacked', *The Advertiser*, 2 September, p.29.

The Advertiser 2000, 'Stolen credit cards used on retailer's web site', 30 August, p.13.

The Economist 2001, 'Stop signs on the web', 11 January, http://www.economist,com/PrinterFriendly.cfm?Story_ID=471742, visited 30 April 2001.

Thompson, D. & Berwick, D. 1998, *Minimum provisions for the investigation of computer based offences*, Report Series 129.1, NPRU, Adelaide.

United Nations (UN) 1999, *International review of criminal policy - United Nations manual on the prevention and control of computer-related crime*, UN, New York, http://www.ifs.univie.ac.at/~pr2gq1/rev4344.html, visited 30 May 2000.

United Nations Asia and Far East Institute for the Prevention of Crime and the Treatment of Offenders (UNAFEI) 2000, *Crimes Related to the Computer Network: Challenges of the Twenty-first Century*, April, Tokyo.

University of Queensland 2001, 'AusCERT notes substantial growth of computer security incidents', 25 January, http://www.uq.edu.au/news/search,asp?method=by Category&c_id=51, visited 12 February 2001.

Van Dijk, S. 2000, 'GST rush at Tax Office exposes security neglect', *Computerworld*, Vol.24 No.2, 10 July, pp.1 & 3.

Verton, D. 2001, 'Technology vendors detail plans to share security information', *Computerworld*, http://www.computerworld.com/cwi/story/0,1199, NAV47_STO56410,00.html, visited 8 February 2001.

Wakefield, J. 1999, 'Internet fraud on the rise', http://www.zdnet.co.uk/news/1999/46/ns-11706.html, visited 18 September 2000.

Walker, J. 1997, 'Estimates of the costs of crime in Australia in 1996', *Trends and Issues*, No.72, Australian Institute of Criminology, Canberra.

Weiss, T. 2000, 'Microsoft says it tracked intruder for 12 days', *Computerworld*, Vol.24 No.18, p.3.

Weiss, M. 2001, 'How the NYPD cracked the ultimate cyberfraud', NYPOST/FOXNEWS, 20 March.