

The Challenges Of Policing Cyberspace

By Commander Barbara Etter, Director, Australasian Centre for Policing Research, Adelaide, Australia

“Safety” is defined in the *Concise Oxford Dictionary* as “being safe, freedom from danger or risks”. Now that most of our lives involve surfing the Net and shopping and communicating via the World Wide Web, we need to feel that it is safe to do so.

The vision for Australasian policing (which includes New Zealand Police), as stated in its strategic directions document,ⁱ is

“A safer and more secure community”

Given that technology, including the Internet, is such an integral part of most of our lives, “community” in the vision statement must equally apply to the new dimension of cyberspace. Police must ensure safety and security in various environments including the home, schools, business and the workplace, whether on-line or off-line, and, in so doing, appropriately address legal, ethical and cultural issues.

The objectives of the paper are to:

- Discuss the risks and dangers of the Internet, as well as the nature of the e-crime problem, its impact on safety in various environments, and the distinct 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 in broad terms what Australasian policing is doing to prevent and reduce the incidence of this type of crime and enhance the safety and security of the community.

Risks and Dangers of the Internet – Is it a Safe Place?

There clearly are a number of dangers or risks involved in utilising the Internet. They include:

- Invasions of privacy;
- Fraud and theft, including the potential use of your credit card details by others to purchase goods and services, and the possibility of identity theft, a fast growing crime;
- Harassment, including spamming, stalking etc;
- Exposure to material considered to be pornographic, violent, hate-filled, racist or generally offensive;
- Ready availability of information to assist people with bomb-making and other dangerous activities;
- Temptation and ability to participate in on-line gambling;
- Vulnerability to exploitation, such as the physical or emotional abuse of children;
- Loss of business and reputation, due to denial of service attacks, web graffiti etc.; and
- Loss of data and damage to systems, through malicious code, such as worms and viruses.

Recent research conducted by the Australian Broadcasting Authority (ABA) found that most adults believed using the Internet involved some risk, with the main areas of perceived risk being:ⁱⁱ

- Financial dangers eg. fraud and credit card number theft (54%);
- Personal data misuse and privacy issues (45%);
- Content exposure concerns (39%); and
- Viruses (21%).

The most common content concern was the perceived risk of children accessing unsuitable content (27%). Access to pornographic material, and the receipt of such content through unsolicited emails or accidental discovery, were the key concerns. The difference in the level of regulation of the Internet compared with other media was the most common theme raised by parents, when asked why they were concerned about access on the Internet.ⁱⁱⁱ The core differences between the Internet and other media, perceived by parents who were more concerned with Internet content, were:^{iv}

- Regulatory differences;
- Monitoring difficulty – individual versus group nature of the viewing;
- The unwanted, unexpected nature of access to unsuitable content; and
- The interactive nature of the medium and the human dimension.

An interesting analogy is that of what is in place to ensure safety on our roads. Whilst the roads can certainly be a dangerous place, there are a myriad of established mechanisms to enhance safety and minimise trauma. These include:

- A system of licensing drivers, registering cars to ensure driver competence and vehicle roadworthiness;
- A complex legislative and regulatory regime which outlines the type of driver behaviour expected on the roads;
- Careful attention to standards, road design and construction, as well as vehicle design, including the provision of air bags, seat belts etc.;
- Regular patrolling of our roads by police officers, including practices such as random breath testing;
- Technological checks and safeguards such as radars, speed cameras, red light cameras, video surveillance;
- Availability of maps, weather forecasts, advisory signs etc. to assist in planning and/or executing journeys; and
- Regular and high profile prosecutions of offenders.

When you compare this to what is in place to ensure safety on the Internet, where admittedly the risk of immediate physical injury or death is usually much lower,^v the situation is quite alarming indeed, particularly when one considers the ease with which one can become a victim.

Criminal behaviour on the Internet, or e-crime,^{vi} presents as one of the major challenges of the future to Australasian law enforcement. As Information and Communications Technology (ICT) becomes even more pervasive, aspects of electronic crime will feature in all forms of criminal behaviour, even those matters currently regarded as more “traditional” offences.

The Environment

As most of us are aware, both Australia and New Zealand have been avid in their uptake of technology. This rapid increase in the use of computer technology has facilitated our participation in the emerging global Information Economy but also increases our exposure to electronic crime issues.

The computer has become an integral part of our way of life, but as our dependency on ICT increases, so too does our vulnerability. This vulnerability was clearly demonstrated in more recent times with:

- The distributed denial of service attacks on Yahoo, eBay and other major Internet players;
- The “Love Bug” virus (or ILOVEYOU worm), Code Red, Nimda and a host of other malicious code;
- The hacking of Microsoft where an attacker apparently gained access to the source code for a future product;^{vii}
- The large scale theft of over a million credit card details from various US e-commerce sites by Russian and Ukrainian crime gangs;^{viii}
- 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;^{ix} 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.^x

Some of these incidents also demonstrate the capacity for a single individual to perpetrate major and widespread criminal harm (with a young Canadian named “Mafia Boy”, the offender in the denial of service attacks, a New York bus boy and high school drop-out allegedly responsible for the large scale ID theft scam and a university student from the Philippines the apparent offender in the Love Bug incident). One can only wonder about the extent of damage that could occur in the case of highly-skilled, well-orchestrated and maliciously motivated attacks.

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.^{xi} It is also estimated that there are some 30,000 websites that post hacker codes which can be downloaded to break passwords, crash systems and steal data.^{xii} The range of easy-to-use tools available to hackers and would-be criminals is astounding.

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. 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.

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 comprehensive 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.

However, 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 8,197 computer security incidents were reported to AusCERT, representing a four-fold increase on the number reported in 1999.^{xiii} Such incidents were commonly either network scans, viruses or distributed denial of service attacks.

The US 2001 Computer Crime and Security Survey^{xiv} 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:^{xv}

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.^{xvi} 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 and reportedly was responsible for the installation of over 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.^{xvii} In addition, we are seeing complex and organised paedophile rings, such as those exposed by Operation Cathedral and Operation Landmark.^{xviii} Operation Cathedral involved a law enforcement operation across 15 different countries against the "Wonderland" paedophile ring and resulted in 1998 in the then largest ever worldwide seizure of paedophile material.^{xix} In Landmark, which was coordinated by the UK's National Crime Squad at the end of 2001, detectives in 19 countries simultaneously targeted 130 people in an operation against persons who used the Internet to download and distribute child pornography.

Computer technology also provides an effective tool for terrorists and foreign intelligence organisations. As James and Cooper state:^{xx}

The Internet provides activists, from the protestor 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.

Thus, we can see that the Internet is populated by a mix of **offenders** ranging from the pimply adolescent in the back bedroom or the practised fraudster, to organised crime and foreign powers. Accordingly people who commit computer crimes vary widely in skills, knowledge, resources, authority and motives.

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 activities on the Internet. It is important to consider youth, not just as potential victims, but to consider ways in which we can prevent their involvement in illegal, inappropriate or delinquent^{xxi} behaviour on the Internet. As one US study on on-line victimisation of youth found, offences and offenders are far more diverse than thought. The problem was not just a case of "adult males trolling for sex". Indeed, much of the offending behaviour came from other youth, including females.^{xxii}

In addition, we are all potential victims and the pool of **victims** has never been larger. The scale of potential victimisation now spans the globe and offenders can access their prey with great ease and at low cost. Particularly vulnerable victims include the elderly, particularly when it comes to fraud, and children. One report commented that young children are "perfect targets" for criminals because they are often "trusting, naïve, curious, adventuresome, and eager for attention and affection".^{xxiii}

One US study found that several characteristics distinguished Internet crimes from other crimes committed against children:^{xxiv}

- Physical contact between the child and the perpetrator does not need to occur for a child to become a victim or for a crime to be committed;
- The Internet provides a source for repeated, long-term victimisation of a child that can last for years, often without the victim's knowledge;
- These crimes transcend jurisdictional boundaries, often involving multiple victims from different communities, states and countries;
- Many victims of Internet crimes do not disclose their victimisation or even realise that they have been victims of a crime.

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. At this point in time, it is difficult to know what is occurring in this area perhaps due to a lack of knowledge about reporting mechanisms, or reluctance, particularly within the private or business sector, to report many electronic crimes to police. (In relation to on-line victimisation of youth, one US study found, for instance, that less than 10% of sexual solicitations and only 3% of unwanted exposure episodes were reported to authorities such as a law enforcement agency, an Internet Service Provider (ISP) or a hotline.^{xxv})

Unique Challenges and Related Response Issues

The nature and particular features of electronic crime will pose new and unique challenges for investigators, because of:

- 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 costs of investigations, which will often be complex and multi-jurisdictional.

Enforcing the law in cyberspace presents significant challenges, particularly in view of rapid technological change. Some of the challenges include:^{xxvi}

- Bridging multi-jurisdictional 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^{xxvii} states that “balancing the need for accountability with the need for anonymity may be one of the greatest policy challenges in the years ahead”.

A major issue which also needs to be dealt with, and which was discussed by the Australian Model Criminal Code Officers Committee,^{xxviii} 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 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.^{xxix}

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, including, at times, real-time tracing.

To date, international harmonisation of the legal categories and definitions of computer crime has been proposed by a number of bodies. 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.^{xxx} 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.

Mutual Assistance (MA) is another area which may be problematic in relation to electronic 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 2 to 3 months. Therefore, this regime cannot be used to provide assistance on a real time or close to real time basis. In effect, one of the very real challenges will be an ability to cut through bureaucratic red tape (where possible and appropriate).

As has been commented, the Internet is the most interlinked and international media the world has ever known. New models will have to be found to bridge the linguistic, cultural and political differences that bear on this issue when it is addressed at a global level.^{xxxi}

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.

The forensic challenges are also significant and foremost among them are:^{xxxii}

- Finding the evidence in the “information ocean”;
- Anonymity;
- Traceability; and
- Encryption.

Data retention by ISP’s and an ability for law enforcement to move quickly to preserve evidence will be essential in this area.

Skills acquisition, 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.

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.

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 national centres for cybercrime to strategically assess, prioritise and task agencies in relation to multi-jurisdictional and complex e-crime matters.

Policing Response

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*.^{xxxiii}

Following on from the scoping exercise, an analysis was undertaken by the Working Party and a strategy developed. 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 is being taken to implement priority taskings, as resources allow. Every effort is being made to ensure that the strategy leverages off a variety of initiatives already in place.

In addition to the response by Commissioners, a multi-agency working party, chaired by the Australian Bureau of Criminal Intelligence (ABCI), is currently examining how best to progress the recommendations from the ABCI's national (law enforcement only) assessment entitled *The Scale of Internet Child Pornography in Australia*. The Working Party includes representatives from the Commonwealth Attorney-General's Department, the Australian Customs Service, ABCI, Australasian Centre for Policing Research (ACPR) and police services. The ABCI national assessment had identified options for law enforcement and highlighted legal considerations and technical limitations which conceal the identities of offenders and limit the capacity of law enforcement to effectively deal with the problem. In general, the assessment found that child sex offenders have embraced information technology to transmit and receive child pornography, network with other offenders and to gain access to potential victims. The assessment identified that a range of improvements were necessary to assist in the investigation and prosecution of Internet child pornography offences.

Clearly, strategic and effective partnerships with the community and the private sector will be absolutely essential to success in the area of Internet crime. 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 be important in responding to the issue and raising the barriers to crime.

Conclusion

The nature of Internet crimes presents complex new challenges for law enforcement with regard to investigating crimes, collecting and analysing evidence, identifying, apprehending and prosecuting offenders, and assisting victims and their families. E-crime is truly a global issue and there will be an unprecedented need for international coordination and cooperation. It will also be important to more fully understand the nature of the problem and to address the significant under-reporting of the phenomenon.

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”. While there will always be a role for traditional investigative techniques, e-crime, however, presents as a new form of business that may require a fundamental paradigm shift in policing. Dealing with the global aspects of the issue will be extremely challenging.

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.

Managing the timely response to, and the investigation of, such crime will indeed be complex and challenging, particularly in an environment of mobile and ubiquitous computing. An effective and holistic response capacity will need to fully embrace prevention and partnership initiatives, including, in relation to on-line victimisation of youth, an emphasis on community education which involves the development of protective behaviours amongst children, educated and involved adults, and effective supervision by parents, teachers and schools. There will also be a need for the development and utilisation of a range of appropriate technologies, as well as the promotion and adoption of strong cyberethics.

We must work together to make our environment, both on and off-line, a safer and more secure place. As one of the Commissioners from the US Commission on Child Online Protection commented:^{,xxxiv}

The Internet changes everything. It upsets our notions of how things should be, how countries should be governed, how companies should be run, how teachers teach and children learn. It mixes up our conceptual framework of what we think we know about the world, about each other and about ourselves. It is liberating, exciting, challenging and terrifying all at the same time ... To a majority of the world's people, the Internet remains mysterious, forbidding, incomprehensible and frightening.

-
- i Australasian Police Ministers' Council, 2000, *Directions in Australasian Policing July 1999 – June 2002*.
 - ii Australian Broadcasting Authority, 2001, *The Internet at Home: a report on Internet use in the Home*, December, Sydney, 6.
 - iii Australian Broadcasting Authority 2001, *The Internet at Home: a report on Internet use in the Home*, December, Sydney, 43.

-
- iv Australian Broadcasting Authority, 2001, *The Internet at Home: A report on Internet use in the Home*, December, Sydney, 42.
- v However, it needs to be realised that attacks against critical infrastructure, such as aviation systems, power grids, traffic systems etc, could indeed result in the loss of life.
- vi The term electronic crime is used to refer to offences where a computer is used as a tool in the commission of the offence, or as a target. It also encompasses the use of a computer as a storage device. Throughout the paper, the terms “computer crime”, “high tech crime”, “digital crime”, “e-crime” and “cybercrime” may be used interchangeably with “electronic crime”.
- vii Gliddon, J, 2000, “Cracks in the armour”, *The Bulletin*, 7 November, 86; Weiss, T, 2000, “Microsoft says it tracked intruder for 12 days”, *Computerworld*, Vol.24 No.18, 3.
- viii Hellaby, D, 2001, “Warning over credit card sting”, *The Australian*, IT section, 20 March, 32.
- ix Legard, D, 2001, “Hackers hit government sites”, *Computerworld*, Vol.24 No.26, 29 January, 12.
- x Weiss, M, 2001, “How the NYPD cracked the ultimate cyberfraud”, NYPOST/FOXNEWS, 20 March.
- xi O’Brien, K, & Nusbaum, J, 2000, “Intelligence collection for asymmetric threats – Part Two”, *Jane’s Intelligence Review*, November, 50-55.
- xii Adams, J, 2001, “The Weakness of a Superpower”, *Foreign Affairs*, May/June.
- xiii 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](http://www.uq.edu.au/news/search.asp?method=by%20Category&c_id=51), visited 12 February 2001.
- xiv 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.
- xv 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.
- xvi Galeotti, M, 2000, “Chinese crime’s global reach”, *Jane’s Intelligence Review*, November, 10-11.
- xvii O’Ballance, E. 2001, “From Sarin to Cyber Warfare: The Aum Doomsday Sect”, *Intersec*, Vol.11 Issue 2, February, 52-53.
- xviii Ananova, 2001, “Ten arrests in largest ever paedophile crackdown” at http://www.ananova.com/yournews/story/sm_460612.html, visited 5 December 2001.
- xix National Criminal Intelligence Service, 1999, *Project Trawler: Crime on the information highways*, London.
- xx James, L, & Cooper, J, 2000, “Organised exploitation of the information super-highway”, *Jane’s Intelligence Review*, July, 52-55.

-
- xxi Bowker, AL, 2001, “The Advent of the Computer Delinquent”, *Police News*, March, 30-34.
- xxii Crimes Against Children Research Center, 2000, *Online Victimization: A Report on the Nation’s Youth*, June, 33.
- xxiii *Internet Crimes Against Children*, 2001, at http://www.ojp.usdoj.gov/ovc/publications/bulletins/internet_2_2001/internet_2_01_5.html, visited 29 November 2001.
- xxiv *Internet Crimes Against Children* at http://www.ojp.usdoj.gov/ovc/publications/bulletins/internet_2_2001/internet_2_01_5.html, visited 29 November 2001.
- xxv Crimes Against Children Research Center 2000, *Online Victimization: A Report on the Nation’s Youth*, June, ix.
- xxvi 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; Rees, Andrew 2000, ACPR Technology Environment Scan, Report Series No: 133.1, Australasian Centre for Policing Research, Adelaide.
- xxvii 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.
- xxviii 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.
- xxix *The Economist*, 2001, “Stop signs on the web”, 11 January, http://www.economist.com/PrinterFriendly.cfm?Story_ID=471742, visited 30 April 2001.
- xxx 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.
- xxxi Commissioner Stephen Balkam (comments from), 2000, *Companion Volume to The Commission on Child Online Protection (COPA), Report to Congress*, October.
- xxxii US Department of Justice, 2001, *Electronic Crime Needs: Assessment for State and Local Law Enforcement*, Washington DC, March.
- xxxiii 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.
- xxxiv Commissioner Stephen Balkam (comments from), 2000, *Companion Volume to The Commission on Child Online Protection (COPA), Report to Congress*, October.

