ASSOCIATION OF CERTIFIED FRAUD EXAMINERS
Pacific Rim Fraud Conference
Sydney, 11 September 2003

Investigating Cybercrime: Barriers and Solutions

Dr Russell G. Smith
Deputy Director of Research
Australian Institute of Criminology

Introduction

Technology has both facilitated and impeded the investigation of crime, particularly crimes involving computing and communications technologies or what is described as cybercrime. On the one hand, computers have enabled vast amounts of data to be searched and analysed quickly and permitted documents and files to be scanned and transmitted across the globe in seconds. On the other hand, the sheer quantity of information creates considerable problems for investigators who sometimes have to examine gigabytes of data and break encryption codes before the material they are interested in can be discovered.

This paper identifies a number of barriers to the effective investigation of cybercrime, and offers some solutions that could be used to streamline future investigations in cyberspace.

The Nature of Cybercrime

For the purposes of this presentation, I'd like to use a broad definition of cybercrime that includes: crimes *committed through the use of* computing and telecommunications technologies (e.g. electronic funds transfers, electronic manipulation of sharemarkets, and the dissemination of misleading advertising information or offensive content); crimes *directed at* computing and communications technologies as the target of the illegality (e.g. computer hacking and vandalism, such as viruses), or theft of telecommunications and Internet services; and crimes in which computing and communications technologies are *incidental*, but nonetheless involved in the commission of crime (e.g. theft of funds by creating fictitious invoices on a company's computer could just as easily be committed on paper, but the opportunity to manipulate paper accounts might not be immediately apparent to an offender, whereas the theft of funds electronically might seem more likely to be successful and not detected. Hence there is a need to consider cases in which the use of a computer was sometimes seen to be of peripheral relevance).

Finally, the discussion is primarily (although not exclusively) concerned with crimes that take place across jurisdictional borders, particularly those that involve offenders and victims (and other parties) located in different countries. This provides a link with the title of "cybercrime" or crime committed in "cyberspace" – which is simply a shorthand expression for the globally networked computers that may be used for criminal purposes.

1. Obtaining Witness Cooperation

The first impediment that faces investigators is that of securing the cooperation of complainants and witnesses. It is now well-documented that the victims of crimes of this nature are reluctant to report them to the police. Ernst & Young found in its most recent 8th Global Survey of business fraud, that only one quarter of frauds reported in the survey were referred to the police and only 28% of those respondents were satisfied with the resultant investigation (Ernst & Young 2003).

Some of the reasons given by the respondents of an Australian survey conducted by Deakin University (1994) in Melbourne of fraud incidents against businesses in Victoria for not reporting fraud to the police included a belief that the matter was not serious enough to warrant police

attention, a fear of consumer backlash, bad publicity, inadequate proof, and a reluctance to devote time and resources to prosecuting the matter. In the case of cybercrime, this last explanation is of great significance as the time and resources needed to prosecute an offender in another jurisdiction can be considerable.

Similar reasons for non-reporting of electronic commerce incidents were given by the respondents to KPMG's *Global eFraud Survey* (2001) in addition to the key factor of the need to re-instate systems quickly so as to prevent loss of business. Reporting the matter to the authorities simply prevented the organisation in question from minimising its financial losses, and possibly leading to further losses being incurred in prosecuting the matter.

Businesses are reluctant to report cybercrime simply due to a fear of 'sending good money after bad' as experience may have led them to believe that it will be impossible to recover losses successfully through legal avenues and that the time and resources which are required to report an incident officially and to assist in its prosecution simply do not justify the likely return on investment. Prosecution may entail countless interviews with the police, extensive analysis of financial records, and lengthy involvement in court hearings for staff.

The result is that investigators may face considerable barriers in securing cooperation from victims and witnesses, especially those located in other countries.

2. Choosing the Appropriate Jurisdiction

Where offences are committed in various countries or where the offender and victim are located in different places, questions arise as to which court should deal with the matter. If the offence in question can be charged in the country in which the offender is located then problems of extradition will be avoided, but if the offence must be charged in the country in which the victim is located or where the effect of the conduct occurred, then the offender will need to be extradited to that country.

A recent case that illustrates this question concerned a resident of Melbourne in Victoria who was accused of stalking a woman in Canada by sending letters and E-mail messages and using the telephone and the Internet. The Canadian woman complained to police in Toronto who referred the case to the Victoria Police. When the case came before a Magistrate in Melbourne, the accused argued that the effect of his activities, if any, was in Canada and not in Victoria and so the court had no jurisdiction to hear the charges. The Magistrate agreed and dismissed the charges deciding that the fear or apprehension had to be experienced in Victoria for Victorian law to apply.

The Director of Public Prosecutions appealed against the decision and the Supreme Court held that the legislation did have extra-territorial effect and that the defendant could be dealt with in Victoria even though the victim was located in Canada (*DPP* v *Sutcliffe* [2001] VSC 43 (1 March 2001, Gillard J).

The problem of so-called 'negative international jurisdiction' also arises. That is, cases that are not investigated because they could be prosecuted in one of many countries, but none wants to take action. There is also the reverse problem of too many countries wanting to prosecute a particularly noteworthy case. What may be needed to deal with this situation is the creation of an international protocol along the lines of the United Nations protocol on negotiating jurisdiction, setting out how jurisdiction is best determined in these cases. Generally, the rule is that if a country refuses to extradite an offender and if it has power to take action, then it should be obliged to do so.

3. Logistical and Practical Barriers

Conducting investigations across national borders raises many practical problems that delay matters and increase cost. Often, for example, investigators have to contact people on the other side of the globe at inconvenient times. Teleconferences are difficult to arrange at times suitable for all concerned.

Documents often need to be translated, particularly if required for diplomatic purposes. This can cost considerable sums and again delays investigations. Witnesses from non-English speaking countries may need the assistance of interpreters which can also be expensive and slow down investigations.

Finally, countries have different priorities in terms of the importance of cybercrime investigations. Economic crimes committed using computers are often at the bottom of the hierarchy of importance in countries where violent crime is prevalent, or where national security interests may be at stake. The result is that requests for assistance in cybercrime cases may simply be given a much lower priority, especially if they have come from a country with no history of cooperative action.

4. Identifying Suspects

One of the foremost problems that face cybercrime investigators is the identification of suspects. Occasionally, this can lead to considerable problems when the wrong person is arrested.

In March this year, a case was reported in the media in England that provides a good example of the problem of trans-national identity-related fraud. The case concerned a 72 year-old man, Derek Lloyd Sykes, whom the FBI were investigating in connection with alleged telemarketing fraud involving millions of dollars in the United States.

Since 1989, Sykes had been making use of the identity of a 72-year old retired businessman from Bristol in the UK, Derek Bond, who had never met Derek Sykes, and had no connection with his alleged crimes at all. The FBI issued a warrant for the arrest of Derek Sykes and this was executed by South African Police in Durban on 6 February 2003 in the name of Derek Bond. Unfortunately, Derek Bond, the retired businessman, who was on holiday with his wife, was arrested instead of Derek Sykes.

The police relied on the fact that the warrant was in the name of Mr Bond, he was the correct age, looked similar, and had the same passport number. Mr Bond was held in custody at police headquarters in Durban until 26 February 2003 when he was released following the arrest of the real suspect, Derek Sykes, the day before in Las Vegas. Mr Bond is now planning to sue the FBI for wrongful arrest and detention for three weeks in South Africa (BBC News 2003).

In cyberspace the problems are even worse. As the cartoon in the *New Yorker* (July 1993, p. 61) observed, 'on the Internet, nobody knows you're a dog'!

Digital technologies enable people to disguise their identity in a wide range of ways making it difficult to know with certainty who was using a computer from which illegal communications came. This problem is more prevalent in business environments where multiple people may have access to a personal computer and where passwords are known or shared, than in private homes where it can often be assumed who the person was who was using the computer because of circumstantial evidence.

On-line technologies make it relatively simple to disguise one's true identity, to misrepresent one's identity, or to make use of someone else's identity. Remailing services can be used to disguise one's identity when sending E-mail by stripping them of identifying information and allocating an anonymous identifier, sometime encrypted for added security. By using several re-mailing services, users can make their communications almost impossible to follow.

Anonymity can also be achieved in cyberspace using less technologically-complex means. Simply purchasing a pre-paid Internet access service from an Internet Service Provider and renting a telephone line from a carrier, each in a false name provides an easy means of achieving anonymity. Free E-mail services offered by some Internet Service Providers provide another means of securing anonymity as the user may simply register using a false name and address. In addition, the use of Internet Kiosks often permits users to send messages without disclosing their true identity. These services may be used for legal reasons associated with enhancing privacy or for illegal reasons such as evading debts or police investigation of criminal activities. At present there are few verification checks made when such services are obtained.

Even E-commerce technologies that make use of public key infrastructures and digital signatures can be manipulated simply by individuals presenting fabricated documents to support a false identity when registering with a Registration Authority in order to obtain their key pair for use in secure transactions. Although the subsequent transaction may be secure from hackers, the identity of the person holding the key may nonetheless be fictitious.

In a recent study of on-line anonymity, Forde and Armstrong (2002) argued that those Internet services that provide the highest levels of anonymity are most likely to be used for criminal purposes. Encrypted E-mail and Internet Relay Chat that provide higher levels of anonymity were found to be preferred by those engaging in on-line paedophile activity and hacking, while the use of the World Wide Web and File Transfer Protocols that provided weaker levels of anonymity tended to be avoided by serious criminals.

Problems of identification also arise when investigating business entities. In New South Wales, a case was investigated in which the offenders copied official Web sites of premier entertainment venues, including the Sydney Opera House, in respect of almost every detail, including theatre layouts and restaurant information. Programs were constantly up-dated to maintain the façade of legitimacy. The crucial difference was that the fictitious site had its own credit card booking arrangement, so that customers' money would be credited to the offender's account. The bogus site for Sydney appeared on the Internet with a similar URL to the genuine site. The offenders created 23 similar sites mirroring opera houses in Europe, including Paris and Vienna. The computer crime unit of the New South Wales Police Commercial Crime Agency contacted the FBI after tracing the bogus site to a Miami Internet server. Since then, the server has re-located to California (Kennedy 2002). Similar problems involving mirror Websites have been reported in Australia against on-line banking sites, although these have been quickly identified and dealt with.

Problems of identifying suspects are usually resolved by traditional investigative techniques, such as the use of video surveillance or gathering indirect circumstantial evidence that locates the accused at the terminal at a particular time and day. However the use of intrusive surveillance is not always successful with attention having to be paid to human rights issues and legal privileges.

Some investigators are beginning to use biometric means of identification. At present, few computers have biometric user authentication systems such as fingerprint scanners when logging-on. When they become more widespread, problems of identification may be reduced, although,

of course, once a person has logged-on, this does not prevent someone else from using that terminal without the person's knowledge if they are absent.

DNA samples can also be gathered from keyboards which have been used to identify an individual with a particular computer in some cases.

The result, then is that it can be extremely difficult to determine precisely who is behind particular cybercrimes.

5. Search and Seizure

Two methods of obtaining data from a computer system can be distinguished on technical and legal criteria. In the first, data are obtained as part of a search of premises or the place where the system is located. The second involves the interception or monitoring of data being transmitted from, to or within the system. This is an important distinction as remote access to computers via the Internet can sometimes result in the search amounting to an interception of telecommunications that needs to comply with special rules concerning warrants.

One recent case involved the investigation of two Russian computer hackers, Vasily Gorshkov and Alexey Ivanov who stole large numbers of credit card details and attempted to extort money from account holders. In an undercover operation, FBI agents posed as representatives of a security firm and made contact with the accused, ostensibly to discuss employment prospects in the United States. The two accused demonstrated their hacking expertise for the agents who then invited them to come to the United States.

While in the United States the FBI agents used a key logging program to discover the accused persons' passwords that would provide access to their computers in Russia. They were then arrested and charged with various offences.

In order to preserve the computer evidence in Russia, the FBI agents immediately copied data from the servers in Russia via the Internet prior to obtaining a search warrant in the United States. The defence raised various objections to this arguing that the search was unconstitutional, being in breach of the Fourth Amendment that requires warrants to be issued prior to searches being conducted. The United States court held that the Fourth Amendment did not apply to these actions as the data had been obtained outside the United States. The court also held that there had been no seizure of the data as it had merely been copied but not read prior to the warrant being obtained (*United States* v *Gorshkov* 2001 WL 1024026, No. CR-550C (W.D. Wash 23 May 2001).

Another problem concerns evidence that is discovered during the course of a search that exceeds the scope of the warrant. In one case, for example, police had obtained a warrant to examine the accused's computer for evidence to support charges of drug dealing, but discovered child pornography on the computer. The police downloaded the 244 JPEG files and charged the accused with possession of child pornography. The court in the United States decided, however, that this evidence had been obtained illegally as it had exceeded the scope of the original warrant (*United States* v *Carey* 172 F. 3d 1268 (10th Cir 1999)).

Difficult problems arise in obtaining digital evidence in cybercrime cases, although in some ways computers have made the process easier through the ability to conduct searches of hard drives remotely via the Internet. Some of the main difficulties, however, relate to obtaining permission to conduct such a search, securing the relevant access device such as a password, decrypting data

that have been encrypted, and imaging a hard drive without interfering with the evidence. There is also the practical problem of conducting searches quickly so that data cannot be removed.

A final problem concerns the retention of material by investigators. If child pornography has been seized by police, they may be unable to return it to accused persons as this would entail the illegal distribution of obscene materials. In the United Kingdom, the *Possession of Unlawful Items Act* could be used to enable police to dispose of child pornography that had been found of computers – but this is not yet in force (see also the *Police Property Act* 1894 (Eng)).

6. Problems of Encryption

A difficult problem that faces cybercrime investigators concerns data that have been encrypted by accused persons who refuse to provide the decryption key or password.

An illustration of the use of strong encryption by a criminal organisation was uncovered during 'Operation Cathedral' by police in 1998, which led to the largest ever global seizure of paedophile material. This involved police in 15 countries who uncovered the activities of the W0nderland (sic) Club, an international network with members in Europe, North America, and Australia who used the Internet to download and exchange child pornography including real-time video images. The Club used a secure network with regularly changed passwords and encrypted content. In Europe alone, over 750,000 images were recovered from computers, along with over 750 CDs and 1,300 videos and 3,400 floppy disks. The encryption used was able to be overcome because one member of the Club cooperated with police and provided access to the files. This led to approximately 100 arrests around the world in September 1998 (Australasian Centre for Policing Research 2000, p. 126).

The other way in which to decrypt data is to install a key logging program onto a computer that will capture the password used for decryption. The installation of such a program, of course, must be done without the knowledge of the accused and a special warrant needs to be obtained for this. In one famous case in the United States, evidence obtained in this way was challenged on the grounds that the key logger involved the illegal interception of wire communications that requires a special warrant. It was held, however, that the key logger only operated when the computer's modem was not connected, thus excluding any interception of telecommunications (*United States* v *Scarfo*, 2001 see: www.epic.org/crypto/scarfo.html).

If all else fails, investigators may seek to break encryption codes, although this is difficult, time-consuming and costly and would be inappropriate in all but the most serious of matters.

Some computer crimes' legislation is beginning to expand the range of investigatory powers available to law enforcement agencies, for example, by making it an offence for a person with knowledge of a computer system to refuse to divulge passwords or to refuse to provide information about encryption. The Australian *Cybercrime Act 2001* (Cth), for example, provides a maximum penalty of six months' imprisonment for failure to comply with a Magistrate's order to provide such information to investigating officials (see s. 3LA *Criminal Code Act 1995* (Cth) and s. 201A of the *Customs Act 1901* (Cth)).

7. Locating and Securing Relevant Material

Considerable difficulties arise in locating and securing electronic evidence as the mere act of switching on a computer may alter critical evidence and associated time and date records. It is also necessary to search through vast quantities of data in order to locate the information being sought.

The Australian Federal Police, for example, has seen an exponential increase in the size of data storage systems that are required to be analysed during investigations. Where a law enforcement examination of a computer hard drive in 1990 involved 50,000 pages of text, a contemporary examination would involve between 5 and 50 million pages of text (Geurts 2000). This increase in investigative capacity has created considerable resource implications for police that will no doubt increase in the years to come.

A major problem concerns the seizure of digital evidence from hard drives on networked computers in which both relevant and irrelevant material (as well as legally privileged material) are contained together. The practical problem arises when imaging hard drives and then having to determine which material is relevant to the charges in question. This creates problems with search warrants where non-specified data are included in the hard drive, arguably leading to the invalidity of the whole search and seizure procedure. It is practically impossible to examine 80GB of data held on a hard drive in order to determine what is relevant. In the United Kingdom the problem of unseparated material seized on hard drives will be resolved when legislative amendments to the *Criminal Justice and Police Act* 2001 come into force.

Other problems relate to disabling networks when seizing data, especially for large public or private sector organisations which rely on 24 hour access to networks, and also the problem of offenders storing data externally on other people's computers in order to evade detection.

8. Mutual Assistance

In order to facilitate criminal investigations carried out internationally, use is often made of mutual assistance treaties. These provide a legal basis for authorities in one country to obtain evidence for criminal investigations at the request of authorities from another country. Instruments of this kind cover a range of assistance including: the identification and location of persons; the service of documents; the obtaining of evidence, articles and documents; the execution of search and seizure requests; and assistance in relation to proceeds of crime. Each year Australia is the originator of over one hundred mutual assistance requests, and receives a further one hundred requests by other nations pursuant to the *Mutual Assistance in Criminal Matters Act* 1987 (Cth).

There are, however, various problems associated with using mutual legal assistance arrangements. The central difficulty is the slow and cumbersome nature of official requests. There are also problems with the direct transmission of documents as mail can only be faxed in an emergency and to a court tribunal. It is also difficult to use direct requests for assistance unless the person seeking assistance knows specifically to whom the request should be sent.

Costs associated with mutual legal assistance are borne by the party providing assistance. This creates hardship where small countries are concerned that are required to process many requests for assistance from large countries, but they rarely seek assistance themselves. This means that such small countries are subsidising the legal process of much larger nations.

Obtaining evidence in cybercrime cases through the use of formal mutual assistance arrangements entered into between nations can be exceedingly slow and ineffective. Often searches need to be conducted immediately in order to preserve evidence held on servers and the prospect of waiting weeks or even months for official diplomatic procedures to be complied with is daunting. Often by the time that assistance has been obtained the trail of evidence has gone cold.

As an alternative to the use of formal mutual assistance arrangements, investigators often rely on informal networks of contacts in different countries established through prior joint investigations

or through contacts made during conferences such as the present. Such good working relationships are crucial to conducting an investigation in a timely and effective way.

9. Securing Extradition

Where an accused person is resident in a country other than the one in which criminal proceedings are to be taken, it is possible for that person to be extradited to that country to stand trial. Extradition requires not only that an appropriate treaty exist between the two countries concerned, but also that the conduct in question be criminalised in both the referring and receiving country. In the case of computer crime this if often not the case.

McConnell International (2000), for example, recently carried out a survey of cybercrime laws in 52 countries and found that 33 of the countries surveyed had not yet updated their laws to address any type of computer crime. Of the remaining countries, 9 had enacted legislation to address five or fewer types of computer crime, and 10 had updated their laws to prosecute six or more of the ten types of computer crime identified.

An example of the kind of difficulties that can arise concerns the case of Onel de Guzman who was alleged to have sent out the so-called 'Love Bug virus' in May 2000. The virus which infected Microsoft Windows operating systems was sent by E-mail attachments which when opened damaged files in the computer and then replicated itself by sending similar messages to all the addresses in the infected computer's address book. The estimated damage caused globally was estimated to be between $6.7 billion and $15.3 billion.

The virus was traced to an Internet Service Provider in the Philippines who cooperated with police to locate the residence in question. A computer science student named Onel de Guzman was arrested but the creation and release of a computer virus was not proscribed by Philippine law at the time. Because the conduct was not illegal in the Philippines he could not be extradited to the United States where the conduct was illegal because of the principle of dual criminality (Bell 2002).

The so-called Citibank case also provides an illustration of the problems associated with securing extradition in cybercrime cases. Between June and October 1994, a group of Russian computer hackers attempted to steal approximately US$10.7 million from various Citibank customers' accounts in the United States by manipulating its computerised funds transfer system.

One offender, Vladimir L. Levin, was working in a Russian firm, and gained access over 40 times to Citibank's funds transfer system using a personal computer and stolen passwords and account identification numbers. Using a computer terminal in his employer's office in St Petersburg, he authorised transfers of funds from Citibank's head office in New Jersey to accounts which he and his co-conspirators held in California, Finland, Germany, the Netherlands, Switzerland, and Israel.

After Levin was identified as a suspect an arrest warrant was issued in a Federal Court in the United States. At the time there was, however, no extradition treaty between Russia and the United States. Levin, however, made the mistake of visiting England to attend a computer exhibition and was arrested at Stansted Airport, in England on 3 March 1995.
There was an extradition treaty between the United States and the United Kingdom but it was necessary to establish that the offences charged in the United States had a counterpart in the United Kingdom. This did not present problems as the offences had equivalents under the Computer Misuse Act (Eng). There was, however, legal argument about whether or not the

United States had jurisdiction to act. It was concluded that there was jurisdiction because the conduct affected magnetic disks located in the United States.

After protracted legal proceedings which went to the House of Lords, he was extradited to stand trial before the Federal District Court in New York's Southern District. On 24 February 1998, he pleaded guilty to conspiracy to defraud and was sentenced to thirty-six months' imprisonment and to pay Citibank US$240,015 in restitution.

Citibank was able to recover all but $240,000 of the $10.7 million worth of illegally transferred funds. None of the bank's depositors lost money and since the fraud was discovered, Citibank required customers to use an electronic password generator for every transfer of funds. The consequences for Citibank's business reputation were, however, considerable (R. v *Governor of Brixton Prison*; *Ex parte Levin* [1996] 3 WLR 657; *In re Levin* House of Lords, 19 June 1997).

Conclusions

How, then, can these problems be overcome? The solutions lie in harmonising laws and procedures globally , improving the technical capabilities of investigators, and finally in sharing information between public and private sector investigators and enhancing international cooperation.

Harmonisation of Laws

The continuing harmonisation of laws and the adoption of international conventions on cybercrime and transnational and organised crime will make prosecutions easier and will greatly improve mutual assistance and extradition of offenders. Already this is starting to occur with the adoption in November 2000 of the United Nations of the *Convention Against Transnational Organised Crime* and the adoption by the Committee of Ministers of the Council of Europe on 8 November 2001 of the *Convention on Cybercrime*. These Conventions contain provisions criminalising certain conduct, as well as provisions dealing with special investigative techniques, witness and victim protection, cooperation between law enforcement authorities, exchange of information, training and technical assistance, and prevention at the national and international levels.

The Australian parliament has recently enacted the *Cybercrime Act* 2001 which commenced operation on 21 December 2001. This Act inserts a new Part into the Commonwealth *Criminal Code Act 1995* and largely follows the provisions of the Council of Europe's *Convention on Cybercrime*. Unfortunately, this legislation applies only to law enforcement agencies and not to corporate investigators and private sector consultants who deal with the vast majority of Australia's cybercrime (Ghosh 2002).

Although the Convention and the *Cybercrime Act* resolve problems to do with copying data from hard drives on premises and remotely, obtaining access to encrypted files, and seizing aggregated data, questions still remain concerning the scope of warrants, the ability to intercept E-mails prior to delivery, data held not on the accused's premises, extra-territorial searches, and the scope of mutual assistance orders (Ghosh 2002).

In addition, there is a need for as many countries as possibly to enact local legislation in order to prevent safe havens from continuing to exist where criminals can base their operations.

Improving Technical Capabilities

The investigation of cross-border cybercrime also requires adequate forensic and technical expertise. This implies the formulation of training programs and the development of investigative

software tools. International training programmes could be developed and expertise could be shared between different nations. The United Nations, under its crime prevention and criminal justice program, could examine the desirability of reviewing its manual on computer crime and further support the work already undertaken by other international organisations. Similarly, the Computer Crime Manual developed by the European Working Party on Information Technology Crime needs to be continually up-dated, particularly with respect to the development of specific software tools used to detect cybercrimes.

The level of funding required for training and also for up-grading equipment is not inconsiderable. This ultimately leads to costs associated with investigations increasing. The result may be that in the future only large-scale criminal activities will able to be investigated, a problem that already exists in many countries.

One solution may be to share the investigatory burden between public and private sector agencies. Already specialist cybercrime units have been established within police services in many countries and as these continue to expand they will become a repository of expertise that the private sector can utilise. Similarly, law enforcement agencies are continuing to outsource specialist forensic tasks to the large accounting consultancy companies who often have former police-trained personnel working for them.

Sharing of Information

Finally, there needs to be greater sharing of information between investigators, both within the public and private sectors. This already occurs in the public sector but openness needs to be encouraged in the private sector as well, even where commercial competitive interests may be at stake. Organisations such as the Association of Certified Fraud Examiners can help to facilitate the exchange of information and to set standards which will enhance the ability to respond effectively to cybercrime.

It is important at the outset for organisations to establish networks of information so that when an investigation begins, contact can be made immediately with the appropriate person in another country. Secure Intranets, such as that used by the Australian Bureau of Criminal Intelligence, are an excellent way in which this can be achieved. Subject to constraints of privacy legislation, these could be used in the private sector as well.

Twenty-four hour computer crime response centres are now being established in many countries. These centres, which are to be used for genuine emergencies only, enable requests for real-time computer investigations to be handled at any time of the day or night in the participating country. In Australia, the Australian Federal Police handles such requests and refers queries to relevant state and territory police services of other Australian Federal Police regional offices.

In the European Union, Europol, which was created in 1998 and based in the Hague, is an information clearing house and analysis centre with law enforcement liaison officers in various member states. It aims to increase cooperation and communication between and among law enforcement agencies in member states rather than acting as a European police service.

The G-8s High-Tech Crime Group, has also recommended the establishment of cooperative arrangements between public sector police and regulatory agencies and the private sector. For example, there is a need for telecommunications carriers and ISPs to make certain information available to investigators on production of an appropriate search warrant. Ideally, such arrangements need to be uniform across jurisdictions. In order to facilitate timely responses to a

request for assistance from another State, the G8 agreed to establish a system of contact points, available 24 hours a day and for 7 days a week ("24/7") which are now in place.

One example of a cooperative venture involving public and private sector bodies is the Cybercrime Unit created by the International Chamber of Commerce's Commercial Crime Bureau in London in 1999. This brings together law enforcement bodies such as Interpol, Scotland Yard, and the FBI, as well organisations within the private sector including major financial institutions and businesses. The Unit acts as a clearinghouse for information on electronic crime and passes details of frauds and solutions between companies and the police.

Throughout the 1990s, a number of initiatives have taken place to address the problem of computer-related crime globally. In the Asia-Pacific region, a Working Group on Information Technology Crime was established in the region which reports to the INTERPOL Steering Committee on Information Technology Crime. In Australia, the Australasian Centre for Policing Research (2001) has devised an *Electronic Crime Strategy* for 2001-03 which presented the views of law enforcement on the control of cybercrime. More recently, the re-structured Australian Crime Commission now includes cybercrime within its jurisdiction over 'serious and organised crime'.

In the United States, the President's Homeland Security Policy and Budget, published under the title *Securing The Homeland, Strengthening The Nation*, has instigated a range of measures to enhance cyberspace security (United States President 2002, pp. 21-23), while the United States 'National Strategy to Secure Cyberspace' sets out a range of measures to secure United States information systems against deliberate, malicious disruption and to foster an increased national resiliency (United States, President's Critical Infrastructure Protection Board 2002, p. 4).

There is, accordingly, an extensive range of initiatives being taken to respond to cybercrime globally. Conferences, such as the present, provide an opportunity for investigators from around the globe to learn of each others' activities in this area. Hopefully, they will make use of the contacts they establish when they resume practice in their home jurisdictions. Armed with the latest information and techniques, we should be well-placed to respond in a timely way to the vast range of challenges that cybercrime has created for the international community.

Acknowledgments
An earlier version of this paper was presented at the Council of International Investigators Conference *East Meets West: Sharing Knowledge and Professionalism* at Perth, Australia, 19 February 2003. I am grateful to Professor Peter Grabosky of the Australian National University for drawing some of the cases referred to in this paper to my attention.

References

Australasian Centre for Policing Research 2000, *The Virtual Horizon: Meeting the Law Enforcement Challenges*, Scoping Paper, Australasian Centre for Policing Research, Adelaide.

Australasian Centre for Policing Research 2001, *Electronic Crime Strategy of the Police Commissioners' Conference Electronic Crime Steering Committee 2001 – 2003*, March. http://www.acpr.gov.au/publications2.asp?Report_ID=103 (visited 18 October 2002).

BBC News 2003, 'Briton May Sue After FBI Bungle', *BBC News Online (UK Edition)*, 26 February.

Bell, R. E. 2002, 'The Prosecution of Computer Crime', *Journal of Financial Crime*, vol. 9 no. 4, pp. 308-25.

Council of Europe 2001, *Convention on Cybercrime*, European Treaty Series No 185, Budapest, 23 November 2001, Council of Europe, Strasbourg http://conventions.coe.int/treaty/EN/projets/projets.htm (visited 29 May 2002).

Deakin University 1994, *Fraud Against Organisations in Victoria*, Deakin University, Geelong.

Ernst & Young 2003, *Fraud the Unmanaged Risk: 8th Global Survey*, Ernst & Young, Global Investigations and Dispute Advisory Services, Johannesburg.

Forde, P. and Armstrong, H. 2002, 'The Utilisation of Internet Anonymity by Cyber Criminals', Paper presented at the International Network Conference, 16-18 July, Sherwell Conference Centre, University of Plymouth, Plymouth. http://www.cbs.curtin.edu.au/Workingpapers/other/Utilisation%20of%20Internet%20Anonymity%20by%20Cyber%20Criminals.doc (visited 29 May 2002).

Geurts, J. 2000, 'The Role of the Australian Federal Police in the Investigation of High-Tech Crimes', *Platypus Magazine: The Journal of the Australian Federal Police*, March, http://www.afp.gov.au/publica/platypus/mar00/intfrd.htm (visited 5 February 2001).

Ghosh, A. 2002, 'The Cybercrime Act 2001: Implementing the European Union's Cybercrime Convention', Paper presented at the RSA Conference, San Jose, 16-22 February.

Kennedy, l. 2002, 'A Scam to Bring the House Down', *Sydney Morning Herald*, 'A Scam to Bring the House Down', 28 August. http://www.smh.com.au/articles/2002/08/27/1030053059530.html (visited 21 October 2002).

KPMG 2001, *Global e.fr@ud Survey*, KPMG Forensic and Litigation Services, Switzerland.

McConnell International 2000, 'Cybercrime and Punishment? Archaic Laws Threaten Global Information'. http://mcconnellinternational.com/services/CyberCrime.htm (visited 30 January 2001).

United States President (George W. Bush) 2002, *Securing the Homeland, Strengthening the Nation*, Office of the President, Washington. http://www.whitehouse.gov/homeland/homeland_security_book.html (visited 30 September 2002).

United States, President's Critical Infrastructure Protection Board 2002, *The National Strategy to Secure Cyberspace (Draft)*, President's Critical Infrastructure Protection Board, Washington. http://www.whitehouse.gov/pcipb/cyberstrategy-draft.pdf (visited 11 October 2002).