



CONTROLLING CROSS-BORDER ECONOMIC CRIME

Dr Russell G Smith
Australian Institute of Criminology

*Paper presented at the
4th National Outlook Symposium on Crime in Australia,
New Crimes or New Responses
convened by the Australian Institute of Criminology
and held in Canberra 21-22 June 2001*

Introduction

Cross-border economic crime can occur in a wide variety of ways. It can involve acts of dishonesty directed at consumers in other countries, manipulation of overseas bank accounts to obtain funds illegally, or fraud directed against governments such as through the evasion of customs duties or taxation when goods are imported from overseas. The laundering of the proceeds of crime also regularly takes place across jurisdictional borders.

The commission of cross-border crime has been greatly facilitated by modern modes of transport, communications, banking, and information processing.

Unlike crimes involving personal violence in which the offender and the victim have to be present together in one place at one time, economic criminals and their victims can be located anywhere in the world—and sometimes never meet in person.

Occasionally, the offender and the victim may be located in one jurisdiction, but the mechanics of the commission of the offence may entail an international component which may give rise to legal problems in determining exactly where the offence occurred, and which country has jurisdiction to deal with it.

On other occasions, there may be multiple offenders located in various jurisdictions who target a number of victims in other jurisdictions and employ strategies in which funds are transferred through still further jurisdictions.

The permutations are limitless.

In order to focus the discussion, the present paper presents four case studies that are illustrative of the problem. They also provide examples of the issues that arise in attempting to control cross-border economic crime in the twenty-first century.

1. One Offender - One Victim

The first situation involves an offender who commits an offence in one country against a victim located in another country. Sometimes even this relatively simple scenario has complications in terms of determining legal jurisdiction.

In the English case of *R. v Thompson* ([1984] 1 WLR 962), for example, the defendant was a computer programmer employed by the Commercial Bank of Kuwait. He opened savings accounts at five local branches of the bank in Kuwait and then programmed the bank's computer to debit various dormant accounts of customers and credit the five accounts he had opened. He then left Kuwait for England where he opened five new accounts with an English bank. He then requested the Kuwaiti bank to transfer the sums in his five Kuwaiti accounts to his English accounts. The Kuwaiti bank transferred about £45,000 in full which he then withdrew.

Thompson was charged in England with six counts of obtaining property by deception. The English Court of Appeal held that he had obtained control of the funds in England rather than Kuwait and so was triable in England. The deception (namely the 'harm' or 'effect' of the crime) had occurred in England when Thompson requested that the funds be transferred from the Kuwaiti bank to the English bank. He was also physically present in England when he received the funds.

2. One Offender - Multiple Victims

The second situation concerns a single offender who deceives multiple victims in other countries. The Internet has greatly facilitated the commission of such crimes.

One recent case concerned a 24 year old man who lived in a Melbourne suburb who manipulated the share price of an American company by posting information on the Internet and sending E-mail messages around the globe that contained false and misleading information about the company.

On 8 and 9 May 1999, he posted messages on Internet Bulletin Boards in the United States and sent more than four million unsolicited E-mail messages, colloquially referred to as spam, to recipients in the United States, Australia and in other parts of the world. The messages contained a statement that share value of the company would increase from the then current price of US\$0.33 to US\$3.00 once pending patents were released by the company, and that the price would increase up to 900 per cent within the next few months. The effect of the information was that the company's share price on the NASDAQ doubled, with trading volume increasing by more than ten times the previous month's average trading volume.

The offender had purchased 65,500 shares in the company through a stock broking firm in Canada several days before he transmitted the information. He sold the shares on the first trading day after the transmission of the information and realised a profit of approximately A\$17,000.

The Australian Securities and Investments Commission prosecuted the offender for distributing false and misleading information with the intention of inducing investors to purchase the company's stock. He pleaded guilty and was sentenced to two years' imprisonment on each of three counts, to be served concurrently. The Court ordered that 21 months of the sentence be suspended upon his entering into a two-year good behaviour bond with a surety of \$500 (*Australian Securities and Investments Commission v Steven George Hourmouzis*, County Court of Victoria, 30 October 2000, Stott J).

3. Multiple Offenders - One Victim

Other cases may involve conspiracy to defraud, in which a number of offenders located in one or a number of jurisdictions target a victim in one of those jurisdictions or some other jurisdiction.

The Citibank case is an example of this. 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.

Levin was arrested at Stansted Airport, in England on 3 March 1995 and, 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).

4. Multiple Offenders - Multiple Victims

Finally, a number of offenders may target a number of victims located in a number of different countries, but employ essentially the same fraudulent strategy.

A good example of this concerns the various advance fee frauds perpetrated by a group of West Africans and others since the 1980s. Various offenders began working from Nigeria targeting victims across the globe. Confederates and other fraudsters in other African countries, the United States, Britain, Canada, Hong Kong, and Japan then began using the same techniques. The scale of these frauds increased considerably and created a global problem for law enforcement. Some prosecutions have taken place in West Africa, the United States and England although many offenders have evaded detection and punishment (Smith, Holmes and Kaufmann 1999).

The United States Secret Service estimated that since 1989, US\$5 billion had been stolen from victims throughout the world, including Australia. Between August and November 1998, Australia Post, in Sydney alone, confiscated 4.5 tonnes of advance fee correspondence which had counterfeit postage, amounting approximately to 1.8 million items. E-mail has proved to be an effective way of disseminating advance fee letters as the true identity of the sender is easy to disguise and original supporting documentation unable to be checked for authenticity.

Prevention and Control

How then, are cases like these able to be prevented and controlled. There are five key approaches that are essential to consider when dealing with cross-border economic crimes of this nature. These are as follows.

1. Providing and Sharing Information

The first approach involves providing information regarding the risks of economic victimisation in order that crime may be prevented, and also freely sharing information widely between regulatory and law enforcement agencies. As Braithwaite and Drahos (2000) argue, the concept of transparency is increasing in its importance in the regulatory debate surrounding globalisation of business. Similarly, transparency should have an important role to play in preventing global economic crime.

Providing and sharing information sounds relatively simple, although in the context of cross-border crime, many practical problems emerge. Language difficulties, geographical distance, lack of knowledge of foreign legal systems, time differences, telecommunications and technological differences, and expense are all likely to impede the effective sharing of information.

Many public sector agencies now provide considerable information regarding fraud victimisation and how to avoid it. Most consumer protection organisations have Websites with information on current scams, as do many police commercial crime agencies and financial services regulators. Global organisations such as the International Organisation of Securities Commissions (IOSC) can also help to provide information and to set standards which are conducive to reducing economic crime.

In July 2000, an important initiative in sharing information occurred when the United States Federal Trade Commission (FTC) entered into an agreement with the Australian Competition and Consumer Commission to provide access to the FTC's *Consumer Sentinel* database of consumer complaints. This now permits regulators in the United States, Canada, and Australia to share information about consumer complaints and to assist each other in cross-border prosecutions - such as those involving Internet sales and on-line auctions.

Operational policing information also needs to be shared between regulatory and law enforcement agencies. In the case of Steven George Hourmouzis, who manipulated the NASDAQ through the use of false E-mail, collaboration was needed between securities regulators in the United States and Australia before a successful prosecution could be mounted.

It is important at the outset for agencies to establish networks of information so that when an investigation begins, contact can be made immediately with the appropriate person in another country's corresponding department. Secure Intranets, such as that used by the Australian Bureau of Criminal Intelligence, are an excellent way in which this can be achieved. They can also be used to share 'Fraud Alert' information and to exchange intelligence needed in investigations.

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 (Geurts 2000). The Australian Federal Police also maintains an extensive overseas liaison network with Federal Agents posted in a number of countries. This clearly facilitates the sharing of information and the operation of mutual assistance.

In another initiative in the United States, the Federal Bureau of Investigation and the National White Collar Crime Centre have co-sponsored the establishment of a central repository for complaints relating to Internet fraud. The Internet Fraud Complaint Centre (IFCC) hopes to ensure that Internet fraud is able to be addressed at all levels of law enforcement (local, state, and federal).

The IFCC was created to identify, to track, and to investigate new fraudulent schemes on the Internet on a national and international level. IFCC personnel collect, analyse, evaluate, and disseminate Internet fraud complaints to the appropriate law enforcement agency. The IFCC provides a mechanism by which Internet fraud schemes are identified and addressed through a criminal investigative effort. The IFCC also provides analytical support, and aid in the development of training modules to address Internet fraud. The information obtained from the data collected provide the foundation for the development of a national strategic plan to address Internet fraud.

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 (Sussmann 1999, p. 480).

In 1996, the G-8 countries established a group of experts ('The Lyon Group') to examine better ways in which to fight international crime. The Group produced forty recommendations that were endorsed by the G-8 heads of state at the Lyon Summit in June 1996. This group has met regularly and has discussed ways of enhancing the ability of law enforcement agencies to investigate and prosecute international crime. In January 1997 it created a sub-group to look specifically at high-technology crime and this sub-group has examined law reform, investigatory, and procedural issues to do with prosecuting cross-border computer crime (Sussmann 1999).

The G-8s High-Tech Crime Group, as it is known, 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.

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.

Cooperative cross-border ventures to deal with money laundering have also been established. The International Money Laundering Information Network (<http://www.imolin.org/organiza.htm>) is an Internet-based network assisting governments, organisations and individuals in the fight against money laundering. IMoLIN has been developed with the cooperation of the world's leading anti-money laundering organisations that include the Commonwealth Secretariat, the Council of Europe, the Financial Action Task Force, Interpol, the United Nations Office for Drug Control and Crime Prevention's Global Programme against Money Laundering, the European Commission, and others. The Egmont Group of the Financial Action Task Force also coordinates the activities of various Financial Intelligence Units globally. In the Asia-Pacific region, anti-money laundering initiatives are coordinated by the Asia-Pacific Group on Money Laundering, while the Council for Security Cooperation in the Asia-Pacific region maintains a Transnational Crime Working Group.

Finally, there is a need for cooperation within the private sector. This is difficult owing to commercial confidentiality requirements, although in the area of fraud prevention, competitiveness is often able to be overcome in the interests of reducing fraud risks in an entire industry. An example of a recent initiative to combat computer abuse, is an alliance that was formed in January 2001 between nineteen of the world's largest information technology corporations. The alliance—the Information Technology Information Sharing and Analysis Centre (IT-ISAC)—is supported by the United States government and seeks to ensure that security threats involving information infrastructures such as the Internet are identified quickly in order for mutually effective solutions to be devised.

Similarly, professional and business organisations need to share information about the risks of economic crime and devise global solutions to facilitate its prevention. Multi-national corporations such as the large accounting and consulting practices have considerable leverage in the business community and are able to identify weaknesses in business systems that may be conducive to the commission of economic crime, and recommend the adoption of appropriate solutions. Their global power is also such that they often represent an authoritative voice in communicating with governments.

2. Encouraging Reporting

The second approach aims at encouraging victims to report incidents of economic crime to regulatory and law enforcement agencies globally—rather than simply accepting the fact of their victimisation and taking no further action.

At present many victims of economic crime simply do not report the matter to the authorities. In KPMG's latest fraud survey conducted in 1999, approximately one third of organisations failed to report frauds to the police (KPMG 1999).

Some of the reasons given by the respondents to Deakin University's (1994) fraud victimisation survey 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 cross-border economic crime, this last explanation is of great significance as the time and resources needed to prosecute an offender in another jurisdiction can be considerable.

Failure to take official action, however, has a number of adverse consequences. Those who have acted illegally may believe that because they have not suffered any adverse consequences from their conduct, they are free to act illegally again in the future, either in exactly the same way in respect of the same victim, or by targeting others employing the same strategy. The West African fraudsters have done exactly this, simply going from one victim to another using the same techniques.

Failure to report and to investigate fraud may also lead to fraud prevention measures being overlooked or their early implementation delayed. The community may also suffer where crime has not been dealt with as incidents will not find their way into official crime statistics and the educative and deterrent effects of publicity in preventing crime will be avoided.

3. Reforming and Harmonising Laws

A third approach involves the reform and harmonisation of laws internationally to permit the effective prosecution and punishment of offenders.

The problems associated with cross-border criminal proceedings are not, however, new and international law has had to cope with the complexities of jurisdictional issues and conflicting substantive and procedural laws for hundreds of years in prosecutions involving sea piracy, slavery, hijacking, war crimes, and other offences that have an international component.

Law reform is essentially a matter for each individual jurisdiction, for as Lord Halsbury LC observed in 1891 in the case of *Macleod v Attorney-General of New South Wales* ([1891] AC 455, 458), 'all crime is local'. This does not mean, however, that parliaments should reform laws in total disregard of reforms introduced elsewhere. In the case of cross-border crime, all aspects of the judicial process would be facilitated if as much uniformity as possible were introduced in relevant laws. This would prevent offenders from 'forum shopping' in which they choose the country with the least onerous legal controls in which to base their activities. It would also enhance uniformity of sanctioning and reduce some of evidentiary difficulties that arise in proceedings.

Achieving uniformity of legislation is, however, neither simple nor quick. In a survey carried out by McConnell International (2000), the laws in 52 countries were examined. Of the countries surveyed, only thirteen (25%) had up-dated their laws relating to computer-related fraud (including Australia).

In Australia, even the harmonisation of domestic criminal laws relating to theft is taking a considerable time to complete and similar delays and problems are being encountered in attempts to harmonise laws governing criminal jurisdiction (Model Criminal Code Officers Committee of the Standing Committee of Attorneys-General 2000).

The growth of computer-related economic crime has, however, given added impetus to the need to harmonise laws relating to economic crime, computer crime, jurisdiction, and procedure, and progress is now being made internationally to achieve this result.

The advent of computer-related crime has meant that a number of countries are now enacting laws with extra-territorial effect—so as to permit prosecutions in respect of crimes and offenders located in some other jurisdiction as long as there is some connection with the country that enacted the law.

In terms of procedural reform, a number of improvements could be made. These include: taking early steps to ensure that evidence and facts are agreed and admitted wherever possible; streamlining interviewing procedures and using teleconferencing technologies for interviewing; using documentary evidence in preference to oral testimony wherever possible; overcoming the barriers to the use of computer-generated evidence; ensuring that evidence is not altered or destroyed before it is able to be obtained from another country; ensuring that police have access to the plain text version of encrypted files, either by requiring the suspect to disclose the encryption key, or by employing trusted third parties to hold copies of private encryption keys which can then be used by law enforcement on production of a warrant.

There is also a need to have appropriate arrangements in place for the apprehension and extradition of suspects to foreign authorities or for their prosecution within the jurisdiction in which they are arrested. Appropriate memoranda of understanding or conventions need to be signed with as many countries as possible participating.

Such agreements and conventions need to deal not only with substantive laws relating to crimes of dishonesty and computer crime, but also jurisdictional and procedural laws concerning mutual legal assistance. In particular laws concerning digital search and seizure need to be consistent and complementary internationally so that police can obtain evidence from computers in other jurisdictions.

The creation of multilateral treaties is not, however, without problems. The Council of Europe's *Draft Convention on Cybercrime* (2000) has taken almost four years to reach its present 5th Revision and it must still be approved by the Parliamentary Assembly—which is expected to take place in April 2001. It must then be revised by the European Committee on Crime Problems—which is expected to take place in December 2001, before it is finally submitted to the Committee of Ministers for adoption—presumably sometime in 2002.

The Convention will, however, be the first international treaty to address criminal law and procedural aspects of various types of criminal behaviour directed against computer systems, networks, or data and other types of similar misuse. As such it will hopefully provide a framework for international reform in this area (Sussmann 1999, Tan 2000).

In November 2000, another milestone was achieved with the adoption by the United Nations of the *Convention Against Transnational Organised Crime*. The Convention is intended to provide a legal framework for concerted action against organised crime, and the basis for the harmonisation of national legislation. It contains provisions requiring the criminalising of certain conduct (including participation in an organised criminal group, money laundering and corruption), as well as provisions on corporate liability, special investigative techniques, witness and victim protection, cooperation between law enforcement authorities, exchange of information on organised crime, training and technical assistance, and prevention at the national and international levels.

The Convention offers great potential for enhanced cooperation among countries with respect to implementation of anti-money laundering measures, confiscation of criminal assets, promotion of extradition and mutual legal assistance mechanisms, and the application of modern technology in the fight against crime.

Allied to the harmonisation of laws, is the need to harmonise other aspects of business practices in order to provide a global environment in which economic crime is difficult to perpetrate and yet simple to detect. Bodies such as the International Accounting Standards Committee (IASC), for example, help to promote uniform accounting practices and procedures within the business community that seek to reduce the risk of improper conduct being engaged in. Similarly, international professional bodies have a role to play in creating uniform ethical practices globally which militate against fraud (Braithwaite and Drahos 2000, p. 121).

4. Training and Resourcing Personnel

The fourth approach involves the provision of training and resources to ensure that police and investigators are able to detect and to investigate crimes effectively.

On a more general level, increasing resources to law enforcement agencies would help to ensure that individuals in the community have confidence in the ability of agencies to investigate and to prosecute allegations of fraud. At present, many cases which are reported are simply unable to be investigated through law enforcement agencies being under-resourced—particularly in relation to the investigation of serious, complex, and time-consuming allegations involving fraud and deception.

The resources provided for the investigation of economic crime generally are often inadequate and the resources given to the investigation of computer-related crime in particular even scarcer. There are also considerable retention problems in ensuring that highly trained police remain in the public sector and are not persuaded to work in the private sector where salaries and conditions are often considerably better. Either governments need to allocate increased budgets for the investigation of economic crime, or else the private sector will need to work cooperatively with law enforcement to conduct its own investigations. This is beginning to occur in Australia with a number of fraud investigators' courses being offered in the private sector - often utilising instructors from police agencies.

Adequate resources also need to be provided for continuous training and for regular up-dating of equipment. The provision of funds for this is problematic. One solution may be for a specified portion of assets confiscated from crime each year to be dedicated to improving training and equipment in this way.

5. Publicising Outcomes

Finally we need to ensure that the outcomes of judicial proceedings are effectively and widely disseminated internationally in order to enhance general deterrent effects on potential offenders.

In the case of white collar offenders who can be said to carry out their activities on the basis of some rational calculation, deterrence remains an important component of fraud control. The confiscation of assets, in particular, represents one of the most effective means of achieving deterrence in the case of economic crime.

Deterrence can best be achieved, however, if offences are reported to the authorities. The media, victims, and regulatory agencies can all play a part in publicising the outcomes of cases. Effective use can be made of the Internet as well as traditional print and electronic media such as television.

The media need to act responsibly, however, in ensuring that these complex cases are reported accurately and without alerting potential offenders to ways in which crime can be committed. Victims such as businesses and financial institutions also have a duty to let the wider public know of the outcome of criminal proceedings in which they have been involved—even if this can entail some negative publicity concerning their own activities or lack of fraud prevention measures within their organisation.

Finally, law enforcement agencies have a role to play in publicising their own activities.

If potential offenders are made aware of the outcome of legal proceedings - particularly financial penalties and orders for the confiscation of assets - they may come to realise that the benefits which they expect to derive from their conduct may not be worth the risks.

Publicity can also inform the public about appropriate fraud prevention measures which can be adopted to prevent victimisation.

Conclusions

The solution to cross-border economic crime lies in the hands of us all, or, as Braithwaite and Drahos (2000) argue, global regulation of business requires active world citizenship. Those included are:

- members of the public who transact business and make use of financial services—who are able to take steps to protect themselves from victimisation;
- businesses engaged in international trade or who may be targeted by overseas criminals—who can adopt various fraud prevention initiatives such as making effective use of the latest information security technologies;
- financial institutions whose electronic funds transfer systems provide opportunities for criminals in other countries to transfer funds illegally, or who may receive the proceeds of crime anonymously from overseas—who can take steps to prevent these problems from occurring and to identify security weaknesses in banking infrastructures;
- regulatory agencies—who have the ability to ensure that those at risk are informed of ways in which economic crime occurs, and who can prevent offenders from acquiring positions of responsibility from which they can perpetrate crimes;
- parliaments and law reform agencies—who can seek to harmonise laws internationally and to ensure that legal and procedural problems of cross-border proceedings are dealt with;
- the media—who can publicise the outcomes of criminal and regulatory proceedings taken against those who perpetrate economic crime; and finally
- police agencies—who can cooperate with each other internationally, ensure that their staff are appropriately trained, and make the most effective use of the resources at their disposal in order to enable action to be taken within their own jurisdictions.

For the future, some of the most pressing issues that need to be addressed include—

- the continuing harmonisation of laws, particularly concerning computer-related crime and the use of electronic commerce, and the adoption of international conventions that seek to control economic and organised crime;
- the need for those jurisdictions that are seen as safe havens for economic offenders to strengthen their laws and procedures in order to make economic crime difficult to commit and to profit from;

- the provision of adequate resources to law enforcement and regulatory agencies to enable appropriately trained staff to be engaged (and retained) for the invariably complex investigations that cross-border economic crime requires;
- and finally, the effective utilisation of the work of the many local and international organisations now involved in controlling cross-border economic crime. It will be important in the future to ensure that these organisations do not duplicate the work of each other and / or produce conflicting strategies to deal with the problem.

Acknowledgments

This paper was first presented at the *International Policing Conference 2001* convened by South Australia Police, the Australian Institute of Police Management, the Australasian Centre for Policing Research, and the Australian Institute of Criminology, Adelaide, 6-8 March 2001.

I am most grateful to Dr Peter Grabosky, Director of Research, Australian Institute of Criminology, for his assistance in the preparation of this paper.

References

- Braithwaite, J. and Drahos, P. 2000, *Global Business Regulation*, Cambridge University Press, Cambridge.
- Council of Europe (2000), *Draft Convention on Cybercrime*, (Draft N° 25 REV.5), European Committee on Crime Problems, Committee of Experts on Crime in Cyber-Space, 22 December 2000, Council of Europe, Strasbourg
(<http://conventions.coe.int/treaty/EN/projets/projets.htm>)
- Deakin University 1994, *Fraud Against Organisations in Victoria*, Deakin University, Geelong.
- Freeh, L. J. 2000, 'Statement for the Record of Louis J. Freeh, Director Federal Bureau of Investigation on Cybercrime Before the Senate Committee on Judiciary Subcommittee for the Technology, Terrorism, and Government Information Washington, D.C. 28 March. <http://www.afp.gov.au/ecrime/louisfreeh.htm> (visited 30 January 2001).
- 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).
- Holland, K. 1995, "Bank Fraud, The Old-Fashioned Way", *Business Week*, 4 September, p. 88.
- Kennedy, D. 1996, "Russian Pleads Guilty to Stealing from Citibank Accounts", <http://catless.ncl.ac.uk/Risks/17.61.html#subj>
- KPMG 1999, *1999 Fraud Survey*, KPMG, Sydney.
- McConnell International 2000, 'Cybercrime and Punishment? Archaic Laws Threaten Global Information'. <http://mcconnellinternational.com/services/CyberCrime.htm> (visited 30 January 2001).
- Model Criminal Code Officers Committee of the Standing Committee of Attorneys-General 2000, *Damage and Computer Offences: Discussion Paper, Chapter 4*, Commonwealth Attorney-General's Department, Canberra.
- Smith, R. G., Holmes, M. N. and Kaufmann, P. 1999, 'Nigerian Advance Fee Fraud', in *Trends and Issues in Crime and Criminal Justice*, No. 121, Australian Institute of Criminology, Canberra.
- Sussmann, M. A. 1999, 'The Critical Challenges from International High-Tech and Computer-Related Crime at the Millennium', *Duke Journal of Comparative and International Law*, vol. 9, no. 2, pp. 451-89.
- Tan, K. H. 2000, 'Prosecuting Foreign-Based Computer Crime: International Law and Technology Collide', paper presented to the *Symposium on Rule of Law in the Global Village*, Palermo, Sicily, 12-14 December.