CHAPTER 3

THE ADEQUACY OF INTERNATIONAL LAW ENFORCEMENT COOPERATION

Introduction

3.1 With the increasingly global nature of crime, assisted by developments in transportation and communications systems, especially the Internet, it is critical that Australia is fully engaged in global law enforcement processes.

3.2 Such international cooperation will extend to working with countries whose legal systems, cultures and philosophies vary greatly from our own. The challenges in harmonising international law enforcement approaches are self-evidently considerable. A simple example relates to capital punishment. Australia does not support the death penalty. It generally refuses to provide mutual assistance to a requesting country in a criminal matter where the person might be subjected to the death penalty if found guilty, and will not extradite such persons. Given that some of our closest South East Asian neighbours impose capital punishment for drug-related offences and those countries are often the source of drugs trafficked into Australia, from whom Australia would wish cooperation in its law enforcement efforts, the issue highlights the potential for difficulties for the international community in readily coming to grips with problems on a global scale.

3.3 In this Chapter, the activities of some of the key multilateral organisations are described and some noteworthy developments highlighted. The Committee is naturally keen to draw lessons from these international deliberations about the adequacy of Australia's approaches to the challenges identified and to assess the appropriateness of Australia's role in the international debates.

The international forums - a brief outline

United Nations

3.4 The United Nations (UN) is the principal and most longstanding vehicle for international cooperation. It has been specifically addressing the issue of crime involving computer and telecommunications technologies actively since 1990. The Eighth UN Congress on the Prevention of Crime and the Treatment of Offenders in that year recommended a series of measures relating to the modernisation of domestic offences, investigative procedures, rules of evidence, forfeiture, mutual legal assistance, the improvement of computer security and the better education of the public and training of officials.[1] And, as recommended by the Eighth Congress, a

1 *Eighth United Nations Congress on the Prevention of Crime and the Treatment of Offenders*, 1990, p. 6.

manual on the prevention and control of computer-related crime was compiled and published in 1994.

3.5 At the Tenth Congress, held in Vienna in April 2000, a Workshop on Crimes Related to the Computer Network was held which addressed in four panel discussions the following topics: the criminology of computer-related crime; problems associated with search and seizure on computer networks; problems associated with the tracing of communications on computer networks; and the relationships between law enforcement agencies and the computer and Internet industries. The Workshop made several recommendations, including calls for greater cooperation between governments and industry and improved international cooperation in tracing offenders.[2]

3.6 The General Assembly, in its resolution 55/59 of 4 December 2000, endorsed the Vienna Declaration on Crime and Justice, committed member states to work towards enhancing their ability to prevent, investigate and prosecute computer-related crime. Resolution 55/63 noted the value, inter alia, of eliminating safe havens for offenders, law enforcement cooperation on international cases, training and equipping of personnel, raising public awareness, and taking into account the need to protect individual freedoms and privacy while preserving the capacity of governments to fight criminal misuse of information technologies.[3]

3.7 The UN also in 2000 adopted a wide-ranging Convention against Transnational Organized Crime and two Protocols thereto, applying only to serious crimes involving organised criminal groups and elements of transnationality. Further workshops have continued to be held on the Convention. For example, a workshop held in Palermo in December 2000 noted that, with the proliferation of technologies on which crime relied, there were concerns about the danger of developing regulations prematurely. It further noted the potential for technological security developments.

3.8 In an earlier development, the United Nations Commission on International Trade Law (UNCITRAL) had developed a Model Law on Electronic Commerce, an international legislative template intended to harmonise domestic legal approaches to e-commerce. According to the submission of the Attorney-General's portfolio, Australia's *Electronic Transactions Act 1999* has adopted the Model Law's approach, structure and key concepts but has adapted it to suit Australian legal traditions and the policy aims of the Australian government.[4] An UNCITRAL Working Group on Electronic Commerce, in whose meetings representatives of the Attorney-General's Department have participated, is developing uniform rules for electronic signatures to

---

2 United Nations Economic and Social Council, Commission on Crime Prevention and Criminal Justice, *Conclusions of the Study on effective measures to prevent and control high-technology and computer-related crime,* Vienna, 2001, p. 6.

3 ibid., p. 7.

4 *Submissions,* pp. 216-217.

provide internationally recognised legislative guidance to countries considering legislation on this topic.[5]

Organisation for Economic Cooperation and Development

3.9 The Organisation for Economic Cooperation and Development (OECD), whose membership consists of 29 technologically advanced countries, including Australia, has taken a leading role in identifying the social and legal implications of new technology. As early as 1969 it created a Data Bank Panel to explore issues related to transborder data flows; which it followed with 1980 *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*. Although non-mandatory, the guidelines were developed to be minimum standards which could be adopted into domestic law by member states and have proved to be highly influential.[6]

3.10 Further non-mandatory guidelines followed. *Guidelines for the Security of Information Systems*, released in September 1992, were significant for their recognition of proportionality - they emphasised that, in determining security measures, the risks to be avoided should be balanced against the cost of the security measures. March 1997 saw the release of *Guidelines for Cryptography Policy* which reasserted the fundamental right of individuals to privacy while also permitting lawful access to plaintext or cryptographic keys of encrypted data. Finally, in December 1999, *Guidelines for Consumer Protection in the Context of Electronic Commerce*, were published which contained the overarching principle that consumers should be afforded no less protection in e-commerce than that afforded in other forms of commerce.

3.11 Australia is an active participant in the OECD's work on e-commerce, including privacy safeguards, consumer protection and authentication.[7] Officers of the Attorney-General's Department have chaired the OECD Working Party on Information Security and Privacy and the OECD Electronic Authentication Steering Group.[8]

Council of Europe

3.12 The Council of Europe (COE) is an intergovernmental organisation formed in 1949 by West European countries. Forty-one European nations are now members. As early as September 1995 it approved a recommendation that:

> Subject to legal privileges or protection, investigating authorities should have the power to order persons who have data in a computer system under

---

5 Attorney-General's Department, *Annual Report 1999-2000,* p. 73.

6 Thomas D. and Loader B.D., eds, *Cybercrime: Law enforcement, security and surveillance in the information age,* Routledge, London, 2000, p. 163.

7 Police Commissioners' Conference Electronic Crime Project Working Party, *The Virtual Horizon: Meeting the Law Enforcement Challenges,* ACPR, Payneham SA, 2000, p. 9.

8 Attorney-General's Department, *Annual Report 1999-2000,* p. 70.

> their control to provide all necessary information to enable access to a computer system and the data therein. Criminal procedure law should ensure that a similar order can be given to other persons who have knowledge about the functioning of the computer system or measures applied to secure the data therein.
>
> Specific obligations should be imposed on operators of public and private networks that offer telecommunications services to the public to avail themselves of all necessary technical measures that enable the interception of telecommunications by the investigating authorities.
>
> Measures should be considered to minimise the negative effects of the use of cryptography on the investigation of criminal offences, without affecting its legitimate use more than is strictly necessary.[9]

3.13 A working group on cybercrime was created by the Council in 1997, which released its first draft convention on 27 April 2000. Several revisions later, the draft was presented to the European Committee on Crime Problems in June 2001 and is scheduled to go to the Committee of Ministers for adoption in September of this year. When completed, it will be open to signature by non-European nations some of which, like the United States, had contributed to the drafting process. The then Minister for Justice and Customs, Senator the Hon. Amanda Vanstone, informed the Committee in January 2001 that, while Australia had not been involved in the drafting of the COE convention, the Attorney-General's Department had been monitoring its development.[10]

3.14 The NCA submitted that the draft convention will be the first international treaty to address criminal law and procedural aspects of various types of offending behaviour directed against computer systems, networks and data.[11] Amongst other things, the convention seeks to create consistency amongst signatory states on the nature and form of legislation criminalising cybercrime, search and seizure of computer data, interception, and to provide mechanisms for mutual legal assistance amongst signatory states.

3.15 Specifically, the convention requires that signatory countries adopt laws requiring government access to encrypted information, criminalising the possession of common security tools and altering wiretapping laws. It is understood that only Malaysia and Singapore have existing laws requiring individuals to release encryption keys and decrypted data to government officials.

---

9 COE, *Recommendation of the Committee of Ministers to Member States Concerning Problems of Criminal Procedure Law Connected with Information,* 1995 [www.privacyinternational.org/issues/cybercrime]

10 *Submissions*, p. 245.

11 ibid., p. 169.

3.16 The Federal Government has recently introduced the Cybercrime Bill 2001 to legislate for new computer offences which was based on the January 2001 Model Criminal Code *Damage and Computer Offences Report* and took into account the draft COE convention.[12] That Bill is currently the subject of inquiry by the Senate Legal and Constitutional Legislation Committee. In his Second Reading Speech on the Bill, the Attorney-General, the Hon. Daryl Williams MP, stated:

> Updated laws are vital if authorities are to effectively detect, investigate and prosecute cybercrime activities. The proposed new computer offences and investigation powers in the [Bill] are a significant development in the fight against these activities and will place Australia at the forefront of international efforts to address the issue of cybercrime.[13]

In relation specifically to the draft COE provision on government access to encrypted information, the Bill provides that a magistrate would be able to order a person with knowledge of a computer system to provide such information or assistance as is necessary and reasonable to enable the governmental officer to access, copy or print data.

European Union

3.17 The European Union (EU) has already taken a number of steps to promote electronic commerce and the use of electronic signatures, and to enhance the security of transactions, following the European Commission's 1998 report to the EU Council on computer-related crime. In 2000, the Council adopted a comprehensive *e*Europe Action Plan which highlights the importance of network security and the fight against cybercrime. In a January 2001 Communication from the European Commission to the Council, several proposals for action were advanced, including the creation of specialist computer crime police units in the 15 member countries, support for appropriate technical training for law enforcement and encouragement of information security action.

3.18 The Commission is currently engaged in developing proposals to harmonise high-tech crime offences among member states and to go further than the draft Council of Europe Convention on Cyber-Crime by ensuring that serious cases of hacking and denial of service attacks are punishable by a minimum penalty in all member states.[14]

3.19 The Commission also indicated its intention to set up an EU Forum in which law enforcement agencies, ISPs, telecommunications operators, consumer representatives, civil liberties organisations and other interested parties could jointly

---

12 House of Representatives, *Hansard,* 27 June 2001, p. 27082.

13 ibid., p. 27081.

14 European Commission, *Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime,* Brussels, 2001, p. 15.

discuss ways to raise public awareness of Internet crime, best-practice security measures and procedures to combat computer-related crime.[15]

Group of 8

3.20 The Group of 8 (G8) comprises the eight leading industrialised countries of the world, namely Britain, Canada, France, Germany, Italy, Japan, Russia and the USA. It was formed as the G7 (without Russia) at an economic summit in France in 1975. A G8 Subgroup on Hi-Tech Crime was formed in 1997. Its activities to date have included the establishment of a network of emergency contacts, the hosting of a computer crime conference for law enforcement personnel, the review of G8 legal systems relating to high-tech crime and examination of the issue of the location and identification of criminals who use networked telecommunications.

3.21 In 1997, the G8 Justice and Interior Ministers issued a *Statement of Principles* concerning electronic crime. These principles included statements against safe havens for criminals, coordination of investigations, training and equipment of law enforcement personnel, protection of confidentiality, development of forensic standards for retrieving and authenticating electronic data. It also suggested that work in this area should be coordinated with the work of other relevant international forums to ensure against duplication of effort.[16]

3.22 In October 1999 the G8 formulated principles on *Transborder Access to Stored Computer Data*, to be implemented through treaties and national legislation. The principles are based on the need for states to establish legal mechanisms which enable them to rapidly access and preserve computer data, on request by another state. Further work is being undertaken on the preservation and disclosure of traffic data, tracing networked communications across national borders, and developing compatible forensic standards for retrieving and authenticating electronic data for use in criminal investigations and prosecutions.[17]

3.23 A G8 conference in Paris in May 2000 considered particularly how governments and industry should interact to counter cybercrime without discouraging the growth of e-commerce. Its outcomes included a recognition of the indispensable nature of international cooperation and the need to ensure that there are no safe havens for cybercriminals, a proposal to require ISPs to store a year's worth of information about the websites visited by subscribers and the email messages they sent, and the

15 European Commission, *Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime,* Brussels, 2001, pp. 2-3.

16 See Police Commissioners' Conference Electronic Crime Project Working Party, *The Virtual Horizon: Meeting the Law Enforcement Challenges,* Payneham SA, ACPR, 2000, p. 66.

17 Attorney-General's portfolio, *Submissions,* p. 227.

establishment of a global, around the clock system of cybercrime contacts.[18] The AFP houses Australia's 24-hour cybercrime response centre.

Financial Action Task Force on Money Laundering

3.24 The Financial Action Task Force on Money Laundering (FATF) is an inter-governmental body whose purpose is the development and promotion of policies to combat money laundering, defined as the processing of criminal proceeds in order to disguise their illegal origin. The aim is to prevent such proceeds from being used in future criminal activity and from affecting legitimate economic activity.

3.25 It was established in 1989 by the G7 countries, with Australia being a founding member. In 1991 the G7 Council of Ministers appointed the then Chairman of the NCA, Mr Justice John Phillips, as FATF President, an honour that was extended to his successor, Mr Tom Sherman. The current membership comprises Australia, Austria, Belgium, Canada, Denmark, Finland, France, Germany, Greece, Hong Kong, China, Iceland, Ireland, Italy, Japan, Luxembourg, the Kingdom of the Netherlands, New Zealand, Norway, Portugal, Singapore, Spain, Sweden, Switzerland, Turkey, United Kingdom and the United States, plus two international organisations, the European Commission and the Gulf Cooperation Council.[19]

3.26 A major initiative of FATF, and one in which Australia played a major role, was the drafting of the *40 Recommendations*, which have become widely accepted internationally as world's best practice anti-money laundering policy guidelines. Those recommendations include:

- each country should criminalise money laundering;
- each country should confiscate proceeds of crime;
- financial institutions should identify customers, not keep anonymous accounts, and maintain identification records for at least five years after the account is closed;
- financial institutions should maintain transaction records for at least five years;
- financial institutions should develop programs against money laundering and should monitor and report on suspect transactions, particularly those involving countries which do not abide by the *40 Recommendations*;
- countries should monitor the physical cross-border transportation of cash and bearer negotiable instruments;

---

18 Police Commissioners' Conference Electronic Crime Project Working Party, *The Virtual Horizon: Meeting the Law Enforcement Challenges,* Payneham SA, ACPR, 2000, pp. 67-68.

19 AUSTRAC, *An Overview of Australia's Anti-money Laundering Strategy,* May 2000, p. 2.

- systems for reporting to a national central agency domestic and international currency transactions over a fixed amount should be set up; and
- there should be administrative cooperation, mutual assistance and extradition cooperation with other countries' appropriate authorities.[20]

3.27 Each member country's own conduct in upholding the *40 Recommendations* is subject to evaluation by FATF and self-assessment exercises by individual countries. Australia's anti-money laundering initiatives to date are outlined in Chapter 2. The 1996 FATF peer review of Australia's performance resulted in a glowing endorsement:

> Australia can pride itself on a well-balanced, comprehensive and in many ways exemplary system, and must be congratulated accordingly. It meets the objectives of the FATF Recommendations and is constantly reviewing the implementation of their anti-money laundering provisions, simultaneously looking well into the future.[21]

3.28 The inter-relationship of financial sectors and the cross-border activities of some criminals and money launderers led to the recognition that it was necessary to promote anti-money laundering activities in the region. As described below, an Asia-Pacific Group on Money Laundering (APG), affiliated with the FATF, was set up with a secretariat in the Sydney office of the NCA in 1997. Similar regional groups have been developed in other regions.

3.29 Since the end of 1998, the FATF has taken a lead in identifying those jurisdictions with rules and practices which impede the fight against money laundering. It devised 25 criteria against which jurisdictions could be assessed and, in a review published in June 2000 after relevant inspections, it named the following 15 countries or jurisdictions as non-cooperative or with serious systemic problems: Bahamas; Cayman Islands; Cook Islands; Dominica; Israel; Lebanon; Liechstenstein; Marshall Islands; Nauru; Niue; Panama; Philippines; Russia; St. Kitts and Nevis; and St. Vincent and the Grenadines. The issues of particular concern included lax customer identity requirements by financial institutions; difficulties in establishing the beneficial ownership of some legal entities; and bank secrecy provisions.[22]

3.30 The FATF offered assistance to help these jurisdictions mend their ways but also warned that, should they fail to make adequate progress in doing so, countermeasures would be applied. It further warned its members that 'financial institutions should give special attention to business relations and transactions with

---

20 FATF, *The Forty Recommendations,* OECD, Paris, (1990).

21 FATF, *Annual Report 1996-97,* 1997, p. 13.

22 FATF, *Review to Identify Non-Cooperative Countries or Territories: Increasing the Worldwide Effectiveness of Anti-Money Laundering Measures,* June 2000.

persons, including companies and financial institutions, from the "non-cooperative countries and territories".[23]

3.31 A second review has recently been completed. Six new jurisdictions have been identified as non-cooperating in the global fight against money laundering (Egypt, Guatamala, Hungary, Indonesia, Myanmar and Nigeria); four countries on the 2000 list have made sufficient progress to be removed from the list (Bahamas, Cayman Islands, Liechstenstein and Panama); progress has been noted in seven jurisdictions though they continue to be listed (Cook Islands, Dominica, Israel, Lebanon, Marshall Islands, Niue, and St Kitts and Nevis); and in three jurisdictions (Nauru, the Philippines and Russia), such inadequate progress has been made that unless significant anti-money laundering legislation is enacted before 30 September 2001, FATF recommends 'the application of further counter-measures which should be gradual, proportionate and flexible regarding their means'.[24] In short, this means that they are not to be black-balled from the international financial system just yet. It is hoped that the counter-measures will go some way to reducing the vulnerability of the international financial system and increase the world-wide effectiveness of anti-money laundering measures.

3.32 Typical of the problems which the FATF wants to counter is the practice of money-raising via the licensing in certain jurisdictions of offshore 'banks' which are poorly supervised and which operate with excessive secrecy provisions. Nauru was found to have about 400 such banks and the Cook Islands seven. Similarly the practice of registering international companies without adequate information about them - and the Cook Islands has some 1200 such companies - is frowned upon, because of the obvious assistance this offers money launderers.

Asia-Pacific Group on Money Laundering

3.33 The Asia-Pacific Group on Money Laundering (APG) was established in 1997. As indicated above, it is one of the regional anti-money laundering groups affiliated with the FATF, with a membership comprising 22 countries from South Asia, South East and East Asia and the South Pacific: Australia; Bangladesh; Chinese Taipei; Cook Islands; Fiji; Hong Kong; China; India; Japan; Macau; China; Malaysia; New Zealand; Niue; Pakistan; Republic of Indonesia; Republic of Korea; Republic of the Philippines; Samoa; Singapore; Sri Lanka; Thailand; USA and Vanuatu. The Sydney-based secretariat was initially funded by Australia as an Asian outreach strategy[25] although now all members of the group contribute.

3.34 The Group's fourth annual meeting was held in Kuala Lumpur, Malaysia, in May 2001. Other regular meetings look at money laundering typologies. The APG

---

23 ibid., p. 12.

24 FATF, *Review to Identify Non-Cooperative Countries or Territories: Increasing the Worldwide Effectiveness of Anti-Money Laundering Measures,* June 2001, p. 4.

25 AUSTRAC, *An Overview of Australia's Anti-Money Laundering Strategy,* May 2000, p. 8.

secretariat serves as a focal point for the coordination of anti-money laundering technical assistance and training in the region.

3.35 The presence of a number of the FATF-listed 'non-cooperative countries and territories' in the APG is clearly a challenge for the group as a whole.

Asia-Pacific Economic Cooperation

3.36 In response to the growing inter-dependence amongst Asia-Pacific economies, the Asia-Pacific Economic Cooperation (APEC) was established in 1989 to promote open trade and economic cooperation amongst its now 21 members. Ten working groups have been established, including one on telecommunications and an Electronic Authentication Task Group.

Council for Security Cooperation in the Asia Pacific

3.37 The Council for Security Cooperation in the Asia Pacific has been described as an unofficial think tank, supporting the ASEAN Regional Forum. Australia is a co-chair, along with the Philippines and Thailand. It supports the Asia-Pacific Working Group on Transnational Crime, in which Australia participates.[26]

Interpol

3.38 Interpol is the shortened title for the International Criminal Police Organization, headquartered in Lyon, France, and the successor to the first international police cooperative body which had been established in Vienna in 1923. It has 178 members worldwide and aims to ensure and promote the widest possible mutual assistance between all criminal police authorities, within the limits of the laws existing in the different countries and in the spirit of the Universal Declaration of Human Rights.

3.39 Interpol's broad objective in relation to computer crime is to enhance law enforcement's international capacity to respond to information technology based crime. Its General Assembly recommended the establishment of five global regions; the first Asian Region (English speaking) Working Party was convened in Melbourne in February 1997. The European Working Party produced the *Interpol Computer Crime Manual*, which has been made available through the Australasian Centre for Policing Research to all Australian police agencies.[27] The AFP is Australia's central reference point for Interpol information exchange, including of computer crime messages. Interpol maintains a database on a secure website of images and operational information on counterfeit payment cards, available to all operational law enforcement agencies and the payment card industry; it is adding to its impressive cross-border art theft intelligence network with cybercrime information.

---

26 Attorney-General's portfolio, *Submissions,* p. 230.

27 Police Commissioners' Conference Electronic Crime Project Working Party, *The Virtual Horizon: Meeting the Law Enforcement Challenges,* Payneham, SA, ACPR, 2000, p. 64.

3.40 As noted in the Preface, the Committee in the 38th Parliament met with the then Secretary General of Interpol, Mr Raymond Kendall, in Canberra in December 1996. The cybercrime issue formed part of the discussion, with Mr Kendall making the observation that such issues were often addressed by the passage of national laws when essentially only an international approach can address international problems of this nature. He noted the signs of positive progress in international law enforcement, such as the adoption by the United Nations in Vienna in 1988 of the *Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances*, which laid the basis for a level of international cooperation on drug trafficking. He had stressed, however, that problems then arise with the practical implementation of such conventions when countries do not act promptly to adapt their national legislation to meet the requirements of the convention.[28]

World Customs Organization

3.41 The Customs Cooperation Council, renamed the World Customs Organization (WCO) in 1994, is an independent intergovernmental body with some 150 member governments worldwide. Its aim is to enhance the efficiency and effectiveness of Customs administrations. Key activities include the development of a law enforcement database, the Customs Enforcement Network, a secure website to provide constantly updated shared data to members. The concept is based on the premise that transnational crime is transborder crime and hence improved Customs communications and intelligence sharing can mean more effective action against transnational crime.[29]

3.42 The WCO also supports a Working Group on Transnational Organised Crime, in which the Australian Customs Service participates.

International Organization on Computer Evidence

3.43 Following the G8's recognition of the need for common computer evidence standards with respect to criminal activity that crosses international borders, the International Organization on Computer Evidence (IOCE) was set up, holding its first meeting in 1993, involving computer forensic experts from the G8 countries. Membership has now been extended to others. The AFP is Australia's representative on the IOCE board.[30]

3.44 IOCE is particularly active in developing standards relating to computer evidence, for ratification by G8 countries. It is also working on issues such as

---

28 See the Committee's February 1997 report entitled *Law Enforcement in Australia - An International Perspective* for a summary of the meeting with Mr Kendall. The transcript of the public hearing held with Mr Kendall on 5 December 1996 can be accessed through the Committee's webpage at http://www.aph.gov.au/nca.

29 Attorney-General's portfolio, *Submissions,* pp. 229-230.

30 Attorney-General's portfolio, *Submissions,* p. 231.

international accreditation and validation of tools, techniques and training in forensic computing.

Australia's participation in international forums

3.45 This above listing of international forums with elements of law enforcement cooperation, while impressive in terms of the sheer volume of activity, is almost certainly not exhaustive. With so much concurrent international activity, the Committee was interested to learn the extent to which Australian law enforcement authorities were involved and, accordingly, the extent to which Australia's concerns were being heard in the international arena.

3.46 The then Minister for Justice and Customs, Senator Amanda Vanstone, assured the Committee that officers posted overseas from the Department of Foreign Affairs and Trade (DFAT), where possible, attended relevant meetings and reported back to the department and law enforcement agencies.[31] The AFP also participates in a number of international forums on electronic crime and reports back to the Australasian Police Ministers' Council and the Heads of Commonwealth Law Enforcement Agencies.[32]

3.47 Given the tyranny of distance and the cost implications of attendance at such conferences, the Committee accepts that maximising the use of locally based DFAT staff is sensible. One obvious drawback, however, is that there must be doubts about the capacity for generalist DFAT officers to contribute meaningfully to technical discussions about law enforcement issues, and to forcefully press Australia's case, rather than to merely act as observers.

Australia's transnational law enforcement relationships

3.48 New technology crime ignores international borders and is becoming adept at exploiting differences in legal systems and gaps in international cooperation. Hence practical international cooperation is vital. Australia's law enforcement relationships with foreign countries are governed by two key pieces of legislation: the *Extradition Act 1988* and the *Mutual Assistance in Criminal Matters Act 1987.*

3.49 The Attorney-General's portfolio submission suggested that Australia's extradition regime had been modernised by the opening up of the kinds of extraditable offences that include computer crime and by the implementation of 'no evidence' extradition arrangements to overcome the problem of differing evidentiary laws between countries.[33]

3.50 The Mutual Assistance in Criminal Matters Act provides the legislative basis for Australia to enter into arrangements with other countries to request and grant

---

31 *Submissions*, p. 245.

32 ibid., pp.245-246.

33 *Submissions,* p. 225.

assistance in criminal matters. Bilateral mutual assistance treaties have been negotiated with a wide range of countries and from 1 March 1997 the Act applied 'passively' to all foreign countries - where appropriate, the Attorney-General can request or grant mutual assistance concerning a particular jurisdiction. The types of assistance covered by the Act include the taking of evidence, the production of documents, the issue of search warrants, the seizure of relevant things, and the freezing, seizure and forfeiture of proceeds of crime.

3.51 The Attorney-General's Department publishes statistics on both extradition and mutual assistance requests by and to Australia. In 1999-2000 Australia made six new extradition requests to other countries and 17 cases were carried forward; six requests were granted and one was refused. Twenty-two new extradition requests were made of Australia and 34 were carried over, in the same period; 13 were granted and 3 refused. Australia made 61 new mutual assistance requests in 1999-2000 and 41 cases were carried forward; of these, 61 were executed and one was refused. In the same period 149 mutual assistance requests were made to Australia and 66 cases carried forward; 122 requests were executed and none was refused.[34]

3.52 There has been a steady upward trend in the number of mutual assistance requests made of Australia over the last four years. In purely numerical terms, Australia 'gives' up to twice as much as it 'receives' though this may not necessarily reflect the amount of work involved. And the process can be exceedingly slow: Swiss authorities provided extensive materials for a particular Australian investigation, into conduct by former directors of Elders IXL Ltd, some nine years after the request was made.[35] This inquiry was one in which the NCA had played a prominent role.

3.53 The deficiencies of the current mutual assistance scheme were addressed in four of the seven submissions received from government/police service representatives of the States and the Northern Territory. The Queensland Minister for Police and Corrective Services, the Hon. Tom Barton, noted:

> Jurisdictional differences in what constitutes a crime inhibits international cooperation at an operational level. While overarching mutual assistance agreements may be in place between jurisdictions, these often require that the grounds on which assistance is sought be defined as a crime both in the requesting country and in the assisting jurisdiction.[36]

3.54 The Victorian Government submitted:

> The effectiveness of the traditional means of cooperation through Mutual Assistance applications is already compromised by administrative delays. The situation is aggravated by technology facilitated crime crossing borders instantaneously. The need to develop and maintain consistent legislation

34 Attorney-General's Department, *Annual Report 1999-2000,* p. 200.

35 ibid., p. 75.

36 *Submissions*, p. 92

> and efficient investigation protocols is becoming more urgent as the methodology used in the commission of crime continues to be influenced by the advent of new technology. [37]

3.55 Northern Territory Police Commissioner, Mr Brian Bates, described the traditional system for making mutual assistance requests as 'cumbersome and lengthy when dealing with electronic crime'[38] while the then Western Australian Police Minister, the Hon. Kevin Prince, conveyed the sentiments of the Computer Crime Investigation Unit in similar terms, that:

> bureaucratic procedures incorporated within the Commonwealth's *Mutual Assistance in Criminal Matters Act 1987* do not facilitate timely intervention in, and resolution of, such [computer crime] criminal matters.[39]

3.56 Mr Prince then gave a detailed account of attempts by his investigators to use alternative international mechanisms, such as Interpol and the International High Tech Crime Contact list, both accessed through the AFP. In one case, a complaint was received by the WA Police Service in November 1999 relating to an extortion attempt via email. Police immediately secured evidence and imaged hard drives. The email header information led to a source Internet Protocol registered to an UK ISP. The ISP complied with a request to preserve the relevant logs for evidentiary purposes. However, the local UK police were reluctant to assist until the request came through official channels. The request was made through formal channels, through the Bureau of Criminal Intelligence within the WA Police Service and Interpol. A short response, insufficient to base further action on, was received over six months later, effectively bringing the inquiry to a halt. Mr Prince noted a second case where no response had been received after three months.[40]

3.57 The frustration expressed at such delays by State/Territory government submitters is, quite clearly, understandable and the Committee notes that the onus is on the Commonwealth Government to seek to take appropriate action to address these concerns.

3.58 It appears that two major impediments exist in the mutual assistance field: limitations on the nature of the investigative assistance that can be offered; and the problems posed by the need for real-time assistance in electronic crime.

3.59 Firstly, Australian law enforcement officers cannot apply for a telecommunications interception or listening device warrant to support a foreign investigation (although if the conduct under investigation might be an offence against Australian law, police could instigate their own investigation). Only certain

---

37 *Submissions,* p. 141.

38 ibid., p. 46

39 ibid., p. 111.

40 ibid., pp. 111-112.

information may be passed to foreign investigators: AUSTRAC data[41] and telecommunications intercept material obtained for an existing Australian investigation.[42] The Attorney-General's portfolio has recognised the problem. It submitted that:

> Based on reciprocity the basic principle which could be considered is that, subject to appropriate controls and safeguards, an investigation tool which is available to support an Australian investigation should also be available to support a foreign investigation into a like offence, unless there is some reason to the contrary…Necessary refinements to the mutual assistance regime to accommodate such developments will be considered, as appropriate.[43]

3.60 Secondly, the instantaneous nature of cybercrime mandates the need for real-time investigation in many cases, so offenders can be caught while still connected electronically. Specifically addressing this issue is clearly the overwhelming demand of submitters to this inquiry.

3.61 As the Attorney-General's submission noted:

> In common with worldwide arrangements, Australia's current mutual assistance regime is geared to the type of investigation which takes place after an offence has been committed and in which the police are attempting to understand what took place after the event. However, this might not be the most effective way to fight e-crime. If investigators are required to wait until the offence is completed, the electronic trail will be cold, computer connections will have been discontinued and the data and the evidence lost.
>
> In a real-time investigation, police would seek to secure admissible evidence of criminal conduct. They would wait until a fresh crime is being committed and then undertake an investigation while the offender is still electronically connected and online so that the relevant messages could be traced back to their source and the offender could be detected red handed.[44]

3.62 Once again, it appears that the Council of Europe's Draft Convention on Cyber-Crime contains appropriate measures to address this problem. Beyond calling for parties to provide traditional forms of mutual assistance and extradition, it also proposes the setting up of a network of 24 hours a day, seven days a week national contact points to speed up international investigations. The NCA's submission drew particular attention to this proposal and expressed its in principle endorsement of the cooperative approach required by the draft convention.[45]

---

41 This is permitted under the *Financial Transaction Reports Act,* s.37A and subsection 27(3A).

42 Permitted under the *Telecommunications (Interception) Act 1979,* paragraph 5B(h).

43 *Submissions,* p. 229.

44 *Submission*s, pp. 228-229

45 ibid., pp. 169-170.

Conclusions

3.63 The Committee has found there to be no shortage of international effort in addressing the need for international law enforcement cooperation to meet the challenges of new technology. That is unquestionably a positive development and one that the Committee welcomes. Equally, there appears to be a fair degree of duplication and little overall coordination, a point noted by the United Nations Commission on Crime Prevention and Criminal Justice.[46] It is worth noting, however, that all discussion at these forums is making a contribution to informing deliberations in Australia, even if there is an element of repetition in its content.

3.64 Australia's participation in these international forums is clearly patchy but - as noted by the Federal Privacy Commissioner with somewhat brutal candour - as a relatively small player on the global scene, Australia may end up at the end of the day having to be a policy taker in this area in order to avoid the adverse consequences of international odium.[47] However, given Australia's respected role in forums such as FATF and its leadership role in taking action to address problems highlighted through international forums, such as in relation to the fight against money laundering, the Committee is confident that its contributions to international deliberations carry sufficient weight to ensure that Australia's interests will at least be given due consideration in the decision-making process.

3.65 In introducing the Cybercrime Bill 2001, the Government has stated that it has taken the Council of Europe's deliberations into account. Given that the intention of the Council's Draft Convention on Cyber-Crime is 'to harmonise national legislation in this field, facilitate investigations and allow efficient levels of cooperation between authorities of different States', and given that such non-European countries as Canada, Japan, South Africa and the United States are active participants in its processes, it appears to the Committee that the Government has made a sensible and pragmatic choice.

3.66 The Committee recognises, however, that the convention is only in draft form and it has not yet been signed. The Committee also notes that some industry and privacy groups in Australia have concerns about aspects of the draft convention which remain to be addressed. Whether the Government's legislation will indeed place Australia 'at the forefront of international efforts to address the issue of cybercrime', as claimed by the Attorney-General, or whether it will prove to be a case of 'premature regulation',[48] will only become clear with the benefit of practical experience.

---

46 United Nations Economic and Social Council, Commission on Crime Prevention and Criminal Justice, *Conclusions of the Study of effective measures to prevent and control high-technology and computer-related crime: Report of the Secretary-General,* Tenth session, item 4, Vienna, May 2001, pp. 16-17.

47 *Submissions*, p. 260.

48 In *Crime in the Digital Age: Controlling Telecommunications and Cyberspace Illegalities* (reproduced in *Submissions*, p. 14) Grabosky and Smith wrote: Current wisdom, in [e-commerce] as in other areas of telecommunications-related crime, is inclined against what might be referred to as premature regulation. Untimely regulatory intervention runs the risk of stifling innovation and product development.

3.67 From the NCA's viewpoint, given that most of its activities have an international dimension, the need for Australia to be fully engaged in the process of international cooperation, whether in the form of mutual assistance, extradition arrangements and purposeful international treaties, has never been greater. Meaningful international cooperation is also dependent, however, on individual nations addressing within their own jurisdictions any unwarranted legal limitations on the forms of assistance that they can offer to their international law enforcement partners. The Committee urges the Government to give priority attention to identifying any such problems, some of which have been described above, and to seek to introduce appropriate remedial measures.