Parliament of the Commonwealth of Australia

PARLIAMENTARY JOINT COMMITTEE
ON THE AUSTRALIAN CRIME COMMISSION

CYBERCRIME

March 2004

ISBN 0 642 71327 8

This document was prepared by the Secretariat of the Parliamentary Joint Committee on the Australian Crime Commission and printed by the Senate Printing Unit, Parliament House, Canberra.

THE COMMITTEE

Members

Hon B Baird MP **(Chair)**

Mr R Sercombe MP **(Deputy Chair)**

Senator K Denman

Senator J Ferris

Senator B Greig

Senator S Hutchins

Senator J McGauran

Mr P Dutton MP

Hon D Kerr MP

Mr C Thompson MP

Secretariat

Mr Jonathan Curtis, Secretary

Ms Anne O'Connell, Principal Research Officer

Ms Rosalind McMahon, Executive Assistant

Parliament House
CANBERRA

Telephone: (02) 6277 3598
Facsimile: (02) 6277 5866
Email: acc.committee@aph.gov.au
Internet: www.aph.gov.au/senate_acc

TABLE OF CONTENTS

CHAPTER 1

INTRODUCTION **1**

Background 1
Duties of the Committee 1
The conduct of the inquiry 2
The report 3
Acknowledgements 3
Note on references 3

CHAPTER 2

CRIME IN CYBERSPACE **5**

What is cybercrime? 5
Crime and the internet 8
Legislation and law enforcement 11

CHAPTER 3

CYBERCRIME AND INTERNET PAEDOPHILE ACTIVITY **23**

The Australian Crime Commission and child sex offences 23
The internet and anonymity 23
Investigating and detecting 30
National register of child sex offenders 34
Conclusion 35

CHAPTER 4

BANKING, CREDIT CARD FRAUD AND MONEY LAUNDERING **37**

The banking industry 37
Internet banking 37
Credit and debit card fraud 40
Identity fraud 43
Money laundering 46
Future directions for banking, credit card fraud and money laundering 48
Conclusion 52

CHAPTER 5

THREATS TO NATIONAL CRITICAL INFRASTRUCTURE 53

What is national critical infrastructure? 53

What are the threats and risks? 54

Preventing infrastructure damage 56

CHAPTER 6

FURTHER DEVELOPMENTS AND CONCLUSION 63

Conclusion and recommendations 64

APPENDIX 1

SECTIONS OF *AUSTRALIAN CRIME COMMISSION ACT 2002* AND *AUSTRALIAN FEDERAL POLICE ACT 1979* 69

APPENDIX 2

LIST OF SUBMISSIONS 71

APPENDIX 3

WITNESSES WHO APPEARED BEFORE THE COMMITTEE AT PUBLIC HEARINGS 73

APPENDIX 4

THE UNITED NATIONS RESOLUTION OF THE GENERAL ASSEMBLY NO. 55/63 "COMBATING THE CRIMINAL MISUSE OF INFORMATION TECHNOLOGIES" 75

APPENDIX 5

CYBERCRIME: COMMONWEALTH LEGISLATION 77

RECOMMENDATIONS

Chapter 2

Recommendation 1 **19**

The Committee recommends that the House of Representatives Committee on Communications, Information Technology and the Arts examine the regulation of Internet Service Providers, including codifying the jurisdictional and evidentiary matters involving material which is transmitted or held by the Provider.

Chapter 3

Recommendation 2 **31**

The Committee recommends that the Government investigate partnerships for establishing a multimedia public education campaign on the risks associated with and the safe use of information technology by children, including parental supervision.

Recommendation 3 **35**

The Committee recommends that the Commonwealth Attorney-General liaises with the State and Territory Attorneys-General to ensure that priority is given to the development and implementation of consistent offence and evidence legislation in relation to cybercrime, which is in accordance with Australia's international obligations.

Recommendation 4 **35**

The Committee recommends that as part of its legislative package to detect and prosecute those who use information technology for the trade of child pornography, the Government introduce a new offence relating to luring and grooming children for sexual purposes.

Chapter 4

Recommendation 5 **40**

The Committee recommends that the Australian Crime Commission in conjunction with the Australian High Tech Crime Centre investigate the provision of general information on fraud trends to financial institutions through a secure subscription based service.

Recommendation 6 **49**

The Committee recommends that the Australian Crime Centre, in consultation with the Australian High Tech Crime Centre (AHTCC), Austrac and other law enforcement agencies give priority to developing a national intelligence gathering strategy for cybercrime in the banking industry. Further the ACC should seek to fill any gaps in intelligence holdings that are identified.

Chapter 6

Recommendation 7 **65**

The Committee recommends that the Government include in its cybercrime strategy, directed training for law enforcement agencies, and the development of a whole of government approach in which individuals can gain expertise which can be shared between those agencies.

Recommendation 8 **66**

The Committee recommends that the Australian Crime Commission continue its current level of involvement in cybercrime investigation, and intelligence gathering, as well as further developing its international liaison role.

Recommendation 9 **66**

The Committee recommends that the Australian Crime Commission ensure its information sharing strategies, including liaison with the Australian High Tech Crime Centre, maximise the opportunities for giving and receiving accurate and timely information about cybercrime methods and technology.

Recommendation 10 **67**

The Committee recommends that the Australian Crime Commission seek out opportunities to participate in appropriate public/private sector cybercrime projects, to promote the sharing of information, and the efficient prevention and investigation of cybercrime offences.

Recommendation 11 **68**

The Committee recommends that the Australian High Tech Crime Centre act as a clearing house for information on cybercrime, in order to explore initiatives to combat it.

Glossary

Chat room An area on the Internet where users can communicate in real time.

Cryptography Encrypting of data so that it is unintelligible.

Cybercrime Criminal activity which uses or takes place through communications technology, including the Internet, telephony and wireless technology.

Hacking Unauthorised access to computer data.

Internet A facility which allows computers to be linked via an international network.

ISP Internet Service Provider – also called Internet Access Providers. (IAPs): a business which sells a service enabling subscribers to use the Internet. The provider's service includes providing software and a phone number. The client also selects a password which allows access to the service. The ISP provides a portal through which all of the client's internet traffic is visible to the ISP. ISPs themselves are connected to one another through Network Access Points (NAPs).

ICH Internet Content Hosts: persons who host Internet content in Australia, or who propose to host Internet content in Australia. Examples include a web farm such as Webcentral or a person who has their own website or server and hosts content provided by a range of contributors. (Source: Internet Industry Association Website at http://www.iia.net.au).

Payload. In communications and information science, a payload is a set of data, such as a data field, block, or stream, being processed or transported, the part that represents user information and user overhead information, and may include user-requested additional information, such as network management and accounting information. (Wiki pedia: http://www.wikipedia.org/wiki/Payload).

SPAM unwanted commercial bulk messages randomly sent to email addresses.

Steganography A process in which illegal data is contained in seemingly innocuous files, such as photographs, which can then be reworked at the destination so as to allow access to the illegal data.

Trojan Trojans are malicious stand alone programs, often sent via an email attachment which, when opened alters or deletes files on the machine, or access emails. It does not replicate nor send itself to other machines.

URL Universal Resource Locator: the address of a website.

Virus A piece of program code. Like a biological virus it copies itself and then attaches to a "host"- another computer program - which can then transfer the virus to other computers, damaging all in its wake. Viruses can be destructive by altering files or erasing information from disks. More seriously they can allow others to gain access to a person's computer without authorisation.

Worms A computer worm is a self-replicating computer program, which unlike the virus does not need to attach itself to another program in order to propagate itself. A worm can delete files, or send email documents.

Chapter 1

Introduction

Background

1.1 On 6 March 2003, the Parliamentary Joint Committee on the Australian Crime Commission agreed to conduct an inquiry into a number of aspects of cybercrime, and the role of the ACC in investigating and detecting it.

1.2 In 2000 the Committee's predecessor, the Parliamentary Joint Committee on the National Crime Authority conducted an inquiry into the Law Enforcement Implications of New Technology.[1] Since that time the complexity of technology has continued to increase exponentially, as have the opportunities for applying technology to criminal activity.

1.3 Of particular concern to the Committee were three areas of increased activity which were incorporated into the terms of reference. The terms of reference were :

That, in accordance with paragraph 55(1)(d) of the *Australian Crime Commission Act 2002*, the Parliamentary Joint Committee on the Australian Crime Commission inquire into and report on recent trends in practices and methods of cybercrime with particular reference to:

1. child pornography and associated paedophile activity;

2. banking, including credit card fraud and money laundering; and

3. threats to national critical infrastructure.

Duties of the Committee

1.4 The Inquiry was conducted under the authority of paragraph 55 (1)(d) of the *Australian Crime Commission Act 2002* (the Act). The paragraph states:

Duties of the Committee
(1) The duties of the Committee are:

(d) to examine trends and changes in criminal activities, practices and methods and report to both Houses of the Parliament any change which the

---

1 Parliamentary Joint Committee on the National Crime Authority 'Law Enforcement Implications of New Technology', August 2001, Available at: http://www.aph.gov.au/Senate/committee/history/index.htm#national

Committee thinks desirable to the functions, structure, powers and procedures of the ACC;

1.5 In developing this Inquiry the PJC considered that the role and capacity of the Australian Crime Commission (the ACC) in this area should be examined to assess any resource implications and the likely effect of cybercrime on the activities and priorities of the ACC.

1.6 The ACC commenced operation on 1 January 2003, replacing the former National Crime Authority. It is established under the *Australian Crime Commission Act 2002*.

1.7 The Commission's role is set out in section 7A of the Act which may be found at Appendix 1.

1.8 At the core of the ACC's investigative role is 'federally relevant criminal activity' which involves 'serious and organised crime'. Section 4 of the Act (see Appendix 1) sets out the characteristics of serious and organized crime, and applies it to a series of offences of which cybercrime is one.

1.9 The inclusion of cybercrime as an offence in the definition of 'serious and organised crime' in the establishing legislation is indicative that the offence is an emerging concern. It was not a matter that was under the purview of the National Crime Authority. In conducting the inquiry the PJC was also interested in establishing the impact of the offence and public awareness of the potential of the crime.

The conduct of the inquiry

1.10 Prior to setting its terms of reference, the Committee received background briefings from the Australian Crime Commission and the Australian Federal Police. These briefings served to provide a context for developing the terms of reference.

1.11 The Committee placed an advertisement in *The Australian* of 9 April 2003, inviting interested parties to provide submissions by 9 May 2003. The Committee readvertised on 7 May 2003 and later extended the deadline for submissions. The terms of reference were also placed on the Committee's website. The Committee also wrote to interested organisations and individuals inviting them to provide a submission to the inquiry.

1.12 The Committee received 35 submissions (including 4 supplementary submissions) and these are listed at Appendix 2. Submissions were placed on the Committee's website for ease of public access.

1.13 The Committee held public hearings in Melbourne on 17 July 2003, in Sydney on 18 July 2003 and in Canberra on 21 July 2003. The hearings included evidence received *in camera*. A list of witnesses who appeared at the hearings is at Appendix 3.

The report

1.14 This report canvasses the principal issues which emerged in evidence and in the submissions provided to the Committee, as they affect the work of the Australian Crime Commission.

1.15 The evidence provided to the Committee represents a snapshot of the application of communications technology in July 2003. As this is not a static area of development, the position is almost certain to be more complex in two years or even less.

1.16 Chapter 2 identifies the principal characteristics and manifestations of cybercrime.

1.17 Chapter 3 addresses the issue of paedophile activity and the Internet, and while the ACC has no direct responsibility for paedophile activity the Commission is involved in a general sense through its investigation of crime which is committed through information technology.

1.18 Chapter 4 examines the extent of, and potential for, criminal interference in cybertechnology within the banking and finance sector. A number of cautionary examples demonstrate some simple precautions which can be taken, as well as surveillance and detection methods. The chapter also discusses the role of organised crime in the banking and finance area.

1.19 Chapter 5 looks at the risks to public infrastructure which is increasingly reliant on communications technology for its operation and maintenance.

1.20 Chapter 6 summarises the main issues and includes recommendations.

1.21 The Committee considered and adopted the report at a private meeting on 11 March 2004.

Acknowledgements

1.22 The submissions were most informative, particularly regarding the technical aspects of cybercrime and were of great assistance to the inquiry and the Committee wishes to thank those individuals and organisations who gave evidence at public hearings and who provided submissions.

Note on references

1.23 References in this report are to individual submissions as received by the Committee, not to a bound volume. References to the Committee Hansard are to the official Hansard.

Chapter 2

Crime in Cyberspace

What is cybercrime?

2.1 The Committee notes that there is no statutory definition of cybercrime.

2.2 The expression 'cybercrime' is a product of the expansion in communications technology which has accelerated over the last twenty five years. A number of definitions of cybercrime was provided to the Committee. The Attorney General's Department defined it as:

> a term that encompasses a variety of offences associated with the use of information and communication technology. The use of the term Cybercrime is synonymous with the term electronic crime (e-crime).[1]

2.3 From the Australian Bankers' Association comes this definition:

> A cybercrime is any crime effected or progressed using a public or private telecommunications service.[2]

2.4 The Australian Crime Commission (ACC) observed that the expressions e–crime, Computer Crime, High Tech Crime, and Cybercrime all refer to the same phenomenon and quotes the definition of e-crime as used by the Australian Centre for Police Research:

> [E-crime includes] offences where a computer is used as a tool in the commission of an offence, as the target of an offence, or used as a storage device in the commission of an offence. [3]

2.5 However, in evidence, the Australian High Tech Crime Centre (AHTCC) distinguished between a definition which focuses on the Internet and one which also includes a number of other technological features

> … we are not concentrating just on the Internet – and cyber is usually referred to as the Internet. We are looking at the misuse of technology in a more holistic sense. The danger is that we will miss other exploits or other criminal activities that fall outside the strict definition of the Internet … . We do not want to limit ourselves to just the Internet, while recognising that the Internet will form the backbone of a whole range of those activities – even things like telephony, with the move to IP telephone systems rather

---

1 Attorney-General's Department, Submission no 21, p.2

2 Australian Bankers' Association, Submission no 19, p.6

3 Australian Crime Commission, Submission no 23, p.6

> than switch systems, are becoming part of the Internet. That is the reason for drawing that distinction.[4]

2.6 The Committee observed that the AHTCC's perspective is not static; it accommodates emerging communications technologies as well as those which are current. The possibilities of mobile phone technology are immense, and the AHTCC's interpretation allows for monitoring developing technology as well as meeting the challenges of that which is current.

A means to an offence

2.7 The definition used by the ACC identifies three kinds of offences which involve the use of communications technology, including the Internet.

2.8 The first kind is an offence which is committed using the technology; effectively it is a conventional crime such as fraud which is committed by technological means.

Computers as targets

2.9 The second kind involves offences which target the computers themselves, and seek to destroy or alter information or data held in them, sometimes with a view to interfering in the processes which that data governs. An example would be an attempt to disrupt a city's water supply by interfering with the computers which control it. The interference can be exercised by a number of means including by hackers, worms, viruses and Trojans.

Hackers

2.10 Hackers are people with sufficient technical ability to gain access to another person's computer or to a network through the use of stolen passwords, or interference technology which provides access to networks and individual computers. It is a recognised and for some, an accepted form of computer activity.

2.11 Symantec's evidence described three different hacking groups:

> The first group are … young kids, 15 to 21 years old, who download the latest hacking tools straight off a web site. If you … go into … any search engine, type in 'hacking tools' and hit return, a plethora of sites come up that will give you the ability to generate your own malicious codes, worms, viruses, hack attacks ... Most of that is filtered out as noise by the technology … They are known vulnerabilities and they are known attacks, so they are fairly easy to block.
>
> The second group would be politically motivated organisations that are attempting to hack into specific countries, for example, organisations that are anti global trade and that sort of thing. You see attacks on high-profile

4 *Committee Hansard,* 21 July 2003 p.24

> commercial organisations launched by special interest groups of that nature on occasions. The final group is … those that are a little more talented in what they do. They … are specifically after personal gain. They … tend to launch the attacks that are not as high profile because you tend not to hear about them. They … are trying to steal credit card information or deploy keystroke loggers without people knowing about it. These things are not designed to bring down infrastructure … or hack into web sites … they are trying to specifically pick up their own information without people knowing. They are … predominantly male, predominantly 15 to 35 years of age.[5]

Worms, viruses and trojans

2.12 The terms 'worm' and 'virus' in relation to computers, are often used interchangeably. However, there are differences between them. A computer worm is a self-replicating computer program, which unlike the virus does not need to attach itself to another program in order to propagate itself. A worm can delete files, or send email documents.

2.13 A virus is a piece of program code, so called because like a biological virus it copies itself and then attaches to a 'host' – another computer program. That program can be another operating system which then transfers the virus to other computers, damaging all in its wake. Viruses can be destructive by altering files or erasing information from disks. More seriously they can allow others to gain access to a person's computer without authorisation.

2.14 Trojans are a stand alone program which does not attach to another program; it does not move from computer to computer on its own, but must be transferred intentionally, such as through email. Trojans are usually malicious: a person can email it with an unremarkable filename and attach a message which, when opened might alter or delete files on the machine, or access emails. As they are transferred deliberately, they generally do not infect other programs and are usually easily deleted.[6]

2.15 Viruses and worms first appeared in the 1980's and Trojans in the mid 70's. With the increasing availability of technology, the opportunities for interference have also multiplied.

Computers as storage

2.16 The third category identified in the definition used by the ACC includes offences in which the computer is used as storage for information about an offence, for example a drug offence in which supply records are kept on computer.

---

5 *Committee Hansard*, 18 July 2003, p.74

6 The definitions of 'worm', 'virus' and 'Trojan' are based on material from the online 'Wikipedia' at: http://www.wikipedia.org.

Crime and the internet

Internet access

2.17 The submission from the Australian Broadcasting Authority (the ABA) notes that the most common Internet access is through a personal computer and a phone line.[7] However, the Authority anticipates that emerging technologies will provide the capacity to access the Internet and other online services using a range of devices, including mobile devices.

2.18 The Australian Bureau of Statistics notes that as at 31 March 2003 there are 4,417,000 household Internet subscribers in Australia. This has increased from 3,486,000 in the March quarter of 2001.[8] The market for those intent on using the Internet for criminal purposes has increased by 37 % in only two years.

2.19 The growth of technology has resulted in a parallel growth of associated criminal activity. Of some concern to the Committee were reports concerning paedophilia, and the ease with which children could be contacted by paedophiles through communications technology. The Committee was also concerned at the extent of the misuse of card technology and the Internet. Advanced telecommunications technology can also threaten the viability of utilities such as electricity and water, and because the Internet knows no international boundaries, this can be achieved from an area remote from the affected facility.

2.20 The Committee noted that the Internet has features which favour criminal activity. They include:

- unregulated establishment of, and access to Internet and email sites;
- anonymity; and
- lack of security and public awareness.

Unregulated establishment and access

2.21 Internet Service Providers are not required to be licensed, and are not regulated except by voluntary codes of conduct. Free email providers such as AOL, Yahoo and Hotmail (all of which operate from outside Australia) require minimal information from the user, making the detection of offenders difficult.

2.22 It is also possible to falsify email software to make an email appear to come from a particular source, but in reality be sent by a third party.[9] One of the most familiar effects of unregulated email is SPAM; these are unwanted emails which may be used to harass, to acquire funds fraudulently (the 'Nigerian' letters in which

---

7 Australian Broadcasting Authority, Submission no 15, p.16

8 Australian Bureau of Statistics publication 8253.0, *Internet Activity*, 1 Sept 2003.

9 PricewaterhouseCoopers, Submission no 12a, pp.25-26

recipients were asked for bank account numbers is an example) or to distribute pornography.

Anonymity

2.23 The Committee noted that Internet and computer criminal activity is supported by the anonymity of the environment. In email, free email services allow the creation of as many different email identities as the user wishes, without any useful information about the identity of that person. In evidence Mr. Gregory Melick observed:

> A short-term fix which would make life a lot easier would be to do away with free Internet accounts such as AOL and Hotmail … because if Internet accounts are not free, people have to pay by credit card, and the vast majority of people who use credit cards have provided appropriate information when obtaining the credit cards and that gives law enforcement some starting point.[10]

2.24 Mr Melick indicated that as far back as 1996 (when there were only 600,000 Internet users in Australia: there are now 7 million) that everybody who used an Internet account should have to go through a 100-point check, the same as if opening a bank account:

> Industry thought the idea was laughable and it had amazing problems, because if we do it in isolation it does not do much about the people in the rest of the world who have access to accounts over there. … In 2000 the United Kingdom had six million [Internet users]; in 2002 it had 10 million. In the United States alone from 1996 to 1997 – that is, from the beginning of 1996 to the end of 1997 – Internet users went from 40 to 100 million … if one does not start doing something about it sooner rather than later we are going to have further problems down the line. France … about two years ago … enacted such provisions.[11]

2.25 The 100 point check system has some drawbacks as the Australian Bankers' Association pointed out.[12] The 100 point check requires provision of original documents, and the increased ability to copy and forge documents easily undermines the integrity of the system, although it is clearly an improvement on no system at all.

Chat Rooms

2.26 Chat Rooms on the Internet were described during the Inquiry as being similar to a conference call on a telephone.[13] Chat rooms use Internet technology to allow a group of people with similar interests to communicate using the one Internet location.

---

10 *Committee Hansard*, 21 July 2003, p.28

11 *Committee Hansard,* 21 July 2003, p. 29

12 *Committee Hansard,* 18 July 2003, p. 45

13 *Committee Hansard,* 18 July 2003, p.15

Access is readily available although in some cases a password might be required. In chat rooms, the participants may also assume identities which are untraceable, or false, which is why these are an ideal environment for paedophiles.

2.27 Chat rooms are an instant form of communication – unlike email which is relayed, and then read. The danger inherent in a chat room is its immediacy and somewhat clandestine nature. Children in particular, can be using chat rooms without their parents being any the wiser – the activity would simply appear in the same way as any typing or entering of text. Although some witnesses indicated it has been possible for police to enter chat rooms to monitor proceedings, gathering evidence in the environment is difficult, time consuming, and may not be cost effective.

2.28 In evidence Symantec Australia indicated that the technological barriers to monitoring chat rooms are not insurmountable:

> If you look at the whole instant messaging or chat room space, … there are a lot of third party solutions out there which you can bolt on to existing instant messaging and chat room technologies to record the conversations. It is just a matter of going out and finding the right bits that fit together and knowing how they work. I do not see that there are any real technology barriers there. It is just an extension of email, which we are all used to and is logged and recorded.[14]

2.29 However, Symantec also informed the Inquiry that there may be some barriers to this because of the increasing use of encryption, which is resource-intensive to decode. The Committee notes from this that although the technology may be available, it may not be feasible to use it for monitoring chat rooms.

Other devices

2.30 There are also devices which can mask the source of information, making it appear that the content is actually from another source.

Security and public awareness

2.31 The evidence showed there are two areas of vulnerability for users of the Internet. One is the potential for access by children to unsuitable content and to features such as chat rooms, and the other is a lack of general awareness of the need to secure a computer. This protects the user not only from nuisance email but also from malicious content (including viruses) and from hacking to obtain details such as Internet banking and on-line shopping transactions.

2.32 The Committee was advised by a number of submitters and witnesses that many parents rely on software filtering programs to protect their children from unsuitable content. These are of varying degrees of usefulness, as the filter tends to eliminate material which appears to be objectionable but which is not. Filters can also

---

14 *Committee Hansard,* 18 July 2003, p.75

do the opposite, and fail to filter very much content at all. There is nothing available at present which will restrict access to sites such as chat rooms.

2.33 Many consumers install virus protection, but do not update it. 'Firewall' programs are available (and are often supplied with computer packages) to assist with blocking malicious content, but consumers either don't install or don't update them, or are unaware that this kind of protection is available.

2.34 The consequences of not having such protection can be serious, as they can be easily attacked by computer hackers, worms and viruses. The virus protection packages are a small expense compared to the havoc which can be caused to personal records, as well as major networks. Even keeping virus and firewall protection up to date does not guarantee full immunity, but most anti virus software companies are able to advise consumers of the latest potential dangers, and the appropriate action to take to minimise damage.

Legislation and law enforcement

2.35 The Attorney General's Department notes in its submission to the Inquiry, there is no single Australian law enforcement or policy body which has responsibility for cybercrime matters. Further, cybercrime enforcement is the responsibility of a diverse group of organisations which include law enforcement, regulatory authorities and research bodies:

> The responsibilities of these organisations are diverse, and in most cases Cybercrime forms only a portion of their work. Each of these entities has different roles ranging from the development and coordination of policy, to the policing and prosecution of crime.[15]

2.36 The submission also observes that there are increasingly significant roles being undertaken by the ACC, and the AHTCC.

The role of the ACC and AHTCC in cybercrime

The ACC

2.37 The *Australian Crime Commission Act 2002* (the Act) sets out the organisation's function. Section 7A (see Appendix 1) sets out the details of its work which includes:

- the collection and analysis of criminal information and intelligence;
- investigative work authorised by the ACC Board on matters relating to 'federally relevant criminal activity'; and
- advising the Board on criminal intelligence priorities and providing strategic criminal intelligence assessments.

---

15 Submission no. 21, p. 17

The Australian High–Tech Crime Centre

2.38 The AHTCC is established as part of the Australian Federal Police. The *Australian Federal Police Act 1979* (the AFP Act) sets out the AFP's role. The relevant sections are set out in section 8 of the AFP Act (see Appendix 1) and include the provision of police services. Police services are defined in the AFP Act as:

> police services include services by way of the prevention of crime and the protection of persons from injury or death, and property from damage, whether arising from criminal acts or otherwise.

2.39 The role of the ACC in relation to cybercrime is similar to the other areas of serious and organised crime mentioned in section 4 of the ACC Act. The ACC is responsive to events which have occurred rather than to those which might occur. Its work is that of a processor of information, an intelligence gatherer, and an operational body which acts on the information and intelligence.

2.40 The AHTCC is sponsored by the AFP and its policing role includes the co-ordination of Australian law enforcement agencies to combat serious crime involving complex technology.[16] This includes:

- providing a national coordinated approach to combating serious, complex and multi-jurisdictional high tech crimes, especially those beyond the capability of single jurisdictions;
- assisting in improving the capacity of all jurisdictions to deal with high tech crime; and
- supporting efforts to protect the National Information Infrastructure.

2.41 The Committee sees the AHTCC's work complementing that of the ACC: the ACC may be said to be primarily an operational organisation, focused on a number of areas of serious and organised crime. The AHTCC is a co-ordinating body which of necessity must have research and analysis resources, in order to provide the support to the state and territory bodies which are its constituents. It is in a position to provide comprehensive information on its particular area of expertise: high tech crime.

2.42 However, in the Committee's view the inter-jurisdictional and international nature of cybercrime demands not only a co-ordinated and unified national strategy but one placed in the international context.

2.43 The Committee notes that much unacceptable Internet activity originates outside Australia, which makes detection and prosecution difficult without some form of international co-operative detection and prosecution system. Tracing and eliminating cybercrime requires a legislative framework that is consistent both domestically and internationally.

---

16 'What is the AHTCC?', http://www.ahtcc.gov.au/

2.44 The ABA, for example, indicated in its submission that a significant proportion of child pornography is produced and/or hosted in Russia and some other Eastern European nations. The Australian Federal Police (AFP) has advised the ABA that 'authorities in these jurisdictions have not attached a high priority to investigating such matters.'[17] The Committee shares the ABA's concern; on an international level it is clear that the commitment to developing a framework for detection and enforcement cannot be assumed, although there are initiatives through The United Nations (Resolution of the General Assembly no 55/63 'Combating the Criminal Misuse of Information Technologies' – see extract at Appendix 4) and, as the Committee was informed by Mr Orlowski, APEC.[18]

2.45 The UN resolution includes recommendations which if implemented would establish a framework for international co-operation creating a responsibility for states to ensure that the misuse of technology can be appropriately investigated, prosecuted and penalised. It also includes the recommendation that the 'general public should be made aware of the need to prevent and combat the criminal misuse of information technologies'.[19]

2.46 In evidence, Mr Orlowski told the Committee of APEC projects following the UN resolution which are designed to assist developing economies:

> [APEC] have done a report on what economies [countries] are doing to implement the United Nations General Assembly resolution. ... At the moment … we are running a workshop to assist developing economies, in particular, to develop cybercrime legislation. At the last count, we had 120 representatives nominated for that workshop, which is quite a large number by APEC standards. That will be followed up by in-country training provided by the United States Department of Justice. They will go to the different economies and work with them to try to get that legislation at least underway by October 2003.[20]

2.47 The Australian arrangements for the areas of UN concern are contained in legislation and in particular, mutual assistance arrangements. The Attorney General's Department submission outlined these.[21] They include the Mutual Assistance Unit in the Attorney-General's Department. The unit has the following functions:

---

17 Submission no 15, p.12

18 APEC is the acronym for Asia Pacific Economic Co-operation. It is a 21 member organisation established in 1989 to further enhance economic growth and prosperity for the region and to strengthen the Asia Pacific community. (http://www.apecsec.org.sg/apec/aboutapec.html)

19 Resolution no 55/63 of the UN General Assembly, 81ST Plenary Meeting, 4 December 2000 (http://ods-dds-ny.un.org/doc/UNDOC/GEN/N00/563/17)

20 *Committee Hansard*, 17 July 2003, p.2

21 Submission no.21, p.15

- Making requests for assistance in criminal matters to foreign jurisdictions on behalf of the Australian law enforcement authorities, including the Australian Crime Commission.
- Coordinating the provision of assistance from other countries for the investigation and prosecution of crime and the restraint and confiscation of assets of crime.

2.48 In addition, the submission advised that Australia is party to a number of bilateral Mutual Assistance in Criminal Matters treaties. Assistance can be provided to countries with which Australia does not have formal treaties, through the *Mutual Assistance in Criminal Matters Act 1987*. This legislation enables Australia to provide assistance on request in relation to taking of evidence, issuing of search warrants, forfeiture, confiscation, or restraining of dealings in property associated with criminal offences, and the recovery of penalties.

2.49 Section 8 of the *Mutual Assistance in Criminal Matters Act 1987* specifically provides that the Attorney General must refuse the requested assistance in cases where the death penalty may be imposed, unless the Attorney is persuaded that special circumstances exist. Cases in which the request may be refused include political prosecutions, and the prosecution of a person for an act or omission that if it had occurred in Australia, would have been an offence under the military law of Australia but not also under the ordinary criminal law of Australia.

2.50 There are several international treaties which affect Cybercrime, including the UN Convention on Transnational Organised Crime, which focuses on international co-operation against crimes such as money laundering. In addition the Council of Europe and the Lyon Group have established networks of law enforcement officers which are operated by Interpol. The AFP is the contact point with this network.[22]

2.51 The Committee also notes that limitations in Australia's domestic legislation prevents assistance being provided to other countries in cases in which telecommunications intercept and listening device material is requested.

2.52 The *Telecommunications (Interception) Act 1979* does not allow Australia to gather intercept and listening device material on behalf of another country. The exception is where the material has already been obtained for an investigation of an Australian offence.[23]

2.53 There are also least 13 Commonwealth Acts of Parliament which have some regulatory relevance to cybercrime (see Appendix 5). In addition, states and territories have their own legislation which is not uniform, either in offence provision or in penalties. The ACC submission gives the example of a lack of uniformity in

22 Submission no.21, pp 7-8

23 Submission no.21, p.15

Commonwealth and State laws as they apply to Internet Content Hosts (ICH)[24] and Internet Service Providers (ISPs). Commonwealth law applies to ICHs but not to content providers, creators or ordinary Internet users. State legislation applies to content providers and ordinary Internet users.[25]

2.54 The state governments focus on the offences which, while they can be committed by electronic means, are 'traditional' criminal offences – for example – fraud, or possession of child pornography. The means to these offences is via a telephone connection, and this is an area of Commonwealth responsibility.

2.55 The Committee notes that there are at least two bodies which could address this lack of consistency, and promote a more focussed and unified approach to the investigation, detection and prosecution of cybercrime. They are: the Standing Committee of Attorneys General, and the Police Ministers' Council.

2.56 The Committee is concerned that while there is no common cybercrime regime in Australia, there is an increasing likelihood of this weakness being exploited by criminal elements.

Internet Service Providers (ISPs) and Internet Content Hosts

ISP's

2.57 Internet Service Providers sell Internet access. The Internet Industry Association website explains the process of providing Internet access. In short, clients require a modem (computer access to a telephone system) and usually enter a contract to pay a monthly fee to use the service. This is usually paid by credit card. The ISP provides software, and a telephone number to provide the Internet access. The client selects a user name and password – which identify him or her to the ISP when access to the Internet is required. The client can then use the World Wide Web, and send and receive email. In addition to serving individuals, ISPs also serve large companies, providing a direct connection from the company's networks to the Internet. ISPs themselves are connected to one another through Network Access Points (NAPs). ISPs are also called IAPs (Internet Access Providers).[26]

2.58 ISP's are not licensed. Anyone (with appropriate information technology skills) can establish themselves as a provider. In this unregulated environment, a number of concerns have emerged.

---

24 The Internet Industry website at http://www.iia.net.au defines Internet Content Hosts as persons who host Internet content in Australia or who propose to do so (this is a similar definition to that in Schedule 5 of the *Broadcasting Services Act 1992*. Examples include a webfarm such as webcentral or a person who has their own website or server and hosts content provided by a range of contributors.

25 Submission no. 23, p.53

26 www.iia.net.au

2.59 The resources of less reputable ISPs can become a storehouse for records of criminal activity. Further there is potential for ISP's to obtain material from client addresses which is confidential, in addition to the credit card payment information which is supplied by the clients when they join the service.

2.60 ISP's are not nationally limited. They can operate from Australia to anywhere in the world, as can international operators operate in Australia. There would be a significant expense for small providers to do this, but it is possible.

2.61 There have been some initiatives in other jurisdictions to minimise the criminal potential associated with ISPs. In evidence Mr. Greg Melick told the Committee that the United Kingdom has legislation which specifies that acts or results occurring in the UK are subject to UK jurisdiction. He continued:

> … until we start enacting appropriate laws, both as to jurisdiction and preservation of evidence, we are not going to get very far.[27]

Internet Content Hosts

2.62 The expression Internet Content Host (ICH) is one which appears to be used in Australia, and few other places. It is defined in Clause 3 of Schedule 5 of the *Broadcasting Services Act 1992* as:

> … A person who hosts Internet content in Australia, or who proposes to host Internet content in Australia.

The Schedule also states that Internet content means information that:

> (a) is kept on a data storage device; and
>
> (b) is accessed, or available for access, using an Internet carriage service;
>
> but does not include:
>
> (c) ordinary electronic mail; or
>
> (d) information that is transmitted in the form of a broadcasting service.

2.63 An Internet Service Provider can also host Internet content, and in practice many do so. These are services which organise and design materials for persons who wish to provide information on the Internet.

2.64 Invitations were extended to Internet Service Providers, and the Internet Industry Association to provide the Committee with a submission to give the Committee an opportunity to hear first-hand what the issues are which are most significant for the service providers and the industry as a whole. None was forthcoming. The Internet Industry Association did provide the Committee with a

---

27 *Committee Hansard* ,21 July 2003, p. 28

copy of the draft code of conduct which is discussed below. However, the Committee had no opportunity to discuss the Code of Conduct or to address associated issues to the industry peak body and industry participants.

Co-operative schemes, and codes of conduct

2.65 The Committee heard that there are international, interdepartmental, Federal/ State government and private sector committees examining the issue of Internet regulation. The Attorney General's Department submission lists no fewer than nine 'cybercrime stakeholders',[28] each of which is working on its own projects involving cybercrime. The submission notes that the Australian Securities and Investments Commission (ASIC) has been working with the Internet Industry Association on a Cybercrime Code of Practice. The association has a wide ranging membership which includes telecommunications carriers, ISPs, e-commerce solution architects, hardware and software vendors and content providers.

The Internet Industry Code of Practice

2.66 The Internet Industry Code of Practice was released by the Internet Industry Association on 21 July 2003, and was provided to the Committee on 8 September 2003. Through self regulation, the Code aims to establish a co-operative working environment between law enforcement agencies (LEAs) and the Internet Industry Association. The code aims to:

- Establish clear guidelines for criminal and civil investigations within the provisions of the *Telecommunications Act 1997* (the Act).
- Establish clear guidelines (within standards of confidentiality and privacy established under the Act) agreed between industry and LEAs as to what constitutes 'such help as is reasonably necessary'. This also is intended to establish public confidence in, and promote the use of the Internet.
- Provide a transparent mechanism for the handling of LEA's investigations for the Internet industry which is clearly understood by both parties.
- Promote positive relations between the LEAs and the Internet industry.
- Give users of the Internet confidence that their privacy and the confidentiality of their transactions will be guarded from unlawful intrusion by LEAs.[29]

2.67 The Committee is concerned about the persuasive effect of the Code. If the Code of Conduct applies only to those who agree to be bound by it, there is still a potential for the problems which the Committee's terms of reference identifies to remain unsolved, as those who wish to operate free of sanctions will still be able to do so.

---

28 Submission no. 21, pp 19-23

29 Internet Industry Code of Practice, paragraph 1.11.

2.68 The Committee considers that the matter of regulation of ISPs should be examined more closely, not only in the context of ensuring the compliance of ISPs with a set of standards, but also in the context of the jurisdictional and evidentiary issues which have emerged in the Internet environment, and which rely on the material held by ISPs.

Recommendation 1

The Committee recommends that the House of Representatives Committee on Communications, Information Technology and the Arts examine the regulation of Internet Service Providers, including codifying the jurisdictional and evidentiary matters involving material which is transmitted or held by the Provider.

2.69 The Committee considers that there is a very strong case for a central co-ordinating body for Cybercrime offences, and a form of regulation which applies to those who refrain from endorsing the Code of Conduct.

Detecting and prosecuting cybercrime

2.70 During the inquiry the Committee became aware of a number of issues that apply generally to the detection of cybercrime and the collection of evidence for prosecution. With anonymising software (which can redirect and divert material), and the ease with which free email addresses can be obtained without supporting identification, detection of cybercrime is difficult and resource intensive.

2.71 The NSW Police also told the Inquiry that it is possible to compromise the actual domain server, 'thereby being able to re-route traffic, say from an Internet banking site.[30] While the Police said this had not actually occurred, the Committee considers it is a possibility which any protective strategy must bear in mind.

2.72 Other methods of masking illegal Internet activity include cryptography and steganography. The former involves encrypting of data so that it is unintelligible; steganography allows illegal data to be contained in seemingly innocuous files, such as photographs, which can then be reworked at its destination so as to allow access to the illegal data.

2.73 One important issue drawn to the Committee's attention was the gathering of evidence in the cybercrime environment. The Committee observed that the in the cyber environment the evidence trail disappears rapidly. There are devices which allow material to be 'scrubbed' from a storage medium; further, as ISPs are not required to retain records, there can be little material left to investigate.

2.74 While it is possible to obtain search warrants to seize computer hard drives, discs and other records, there appears to be no legal way in which Internet activity can

30 *Committee Hansard,* 18 July 2003, p.83

be monitored in 'real time' as can be done with an authorised telephone intercept device, obtained under the *Telecommunications (Interception) Act 1979* (Cth).

2.75 The ACC suggested in its submission[31] that the powers available under section 25A of the *Australian Security Intelligence Organisation Act 1979* (the ASIO Act) might also be made available to the ACC in cybercrime investigations (although in giving evidence in Sydney the ACC clarified this and indicated that this was one possibility among many for the future).[32] These powers would allow real time surveillance of computer based activity to search computer data for a period up to 6 months. The ACC proposed that this – as with the ASIO legislation – would be subject to the issuing Minister being satisfied on reasonable grounds that the intelligence collection will be substantially assisted by the content which is obtained under the warrant.

2.76 The ACC did not press this, and explained that:

> … we are just scoping into the future of electronic policing requirements maybe five or 10 years away. We are not saying that the ACC should have these powers; we are just saying that this is another law enforcement tool that in the future may be directly related to electronic crime investigation.[33]

2.77 The powers suggested effectively offer a licence to hack into other computers. The ACC presented the argument that:

> Such a monitoring warrant enables law enforcement to use investigative tools … to intercept and collect the communications of the subject of the warrant while ignoring those communications which the authorisation to intercept does not cover.
>
> Analogous to telephone intercept warrants in all material respects computer monitoring warrants, issued subject to the same administrative and judicial requirements and safeguards as telephone intercept warrants – would significantly enhance the investigative tool kit available to law enforcement.[34]

2.78 The Committee notes that the provisions of section 25A of the ASIO Act are very limited in their application: they apply only to instances where national security is threatened. There was some discussion during the hearings as to whether powers such as this were appropriate in this context, or whether they should be limited to the provisions of the ASIO Act.

2.79 The practicalities and likely benefits were canvassed in evidence by Mr Gregory Melick, who told the Inquiry:

---

31 Submission no.23, p.55

32 *Committee Hansard*, 18 July 2003, p.5

33 *Committee Hansard,* 18 July 2003, p.5

34 Submission no 23, pp.55-56

> Most of your relevant data and evidence for law enforcement purposes will come from computer hard drives. Once you get that information, you then should be able to go to the various Internet providers to get the preserved data to get your evidentiary trail to lead you to the perpetrator … To randomly try to pluck something out of the ether and interpret it to see what is going on will be almost impossible. You also have the other problems of encryption and steganography.[35]

2.80 The proposed warrants were for telecommunications devices. However, as was pointed out to the Committee, wireless technology, which is not covered by the telecommunications legislation, is being used increasingly in communications.[36] In his submission Mr. Steve Orlowski said

> … failure to develop secure wireless products and applications could raise public concerns over wireless security and slow the spread of this potentially valuable new technology. Economic progress and the strengthening of cyber-security require addressing these concerns.

2.81 Accordingly, any regulating of the Internet environment must account for those who will use wireless technology as well as telecommunications.[37]

2.82 The Committee notes that the need for continuous legislative review, in the light of operational information is fundamental to the detection and prosecution of cybercrime.

Privacy

2.83 The Committee noted that there was some concern regarding privacy and the collection of evidence. In their submission to the Inquiry, Electronic Frontiers said:

> We are concerned … by the increasing prevalence of legislative proposals and laws concerning the Internet that fail to contain an appropriate balance between individuals' privacy and the legitimate needs of law enforcement agencies.[38]

2.84 In evidence to the hearing, the AHTCC indicated that it is aware of the need to balance the right of individuals to privacy of communications and the right of individuals to be protected against criminal activities.[39] A similar sentiment was expressed by ASIC which has been involved with other agencies in advising the

---

35 *Committee Hansard,* 21 July 2003, p.32

36 *Committee Hansard*, 17 July 2003, p.13

37 Mr Steve Orlowski, Submission no 9, p.17

38 Submission no 4, p.3

39 *Committee Hansard*, 21 July 2003, pp.19-20

Internet Industry Association on its proposals for a code of practice which seeks also to address the privacy issue. [40]

2.85 The Committee noted that there is an overall tension between the preservation of privacy and protection of children from unsuitable content and consumers generally from unwanted emails and from malicious material such as viruses.

Technological development

2.86 It has become clear to the Committee that crime authorities must be able to keep pace with the advance of technology. The latest (at the time of writing) 'g3 technology' which allows the mobile telephone to become a portable multi media device will require a reconsideration of the differentiated approaches to the regulation of single function devices.

2.87 The Committee observed that organised crime is well able to fund its own development in this area, for obvious reasons. Further, advances in communications technology enhance the ability of criminal groups to organise themselves at an international level.

2.88 Law enforcement will usually be in a reactive rather than an active position, but the Committee considers that with the right strategic development, agencies will be well placed to at least meet, if not anticipate the increasing challenges of rapid technological development. There appears to be a considerable amount of work being undertaken: there is legislation being prepared by the Attorney General's Department, numerous Committees and interagency discussions, but the Committee considers that this activity needs a well resourced co-ordinating body. The following chapters detail examples which illustrate this more clearly.

40 *Committee Hansard,* 21 July 2003, p. 39

Chapter 3

Cybercrime and Internet Paedophile activity

The Australian Crime Commission and child sex offences

3.1 The Australian Crime Commission (ACC) observed in evidence to the Inquiry that while child sex offences and Internet pornography are not directly an ACC area of operation, the ACC co-ordinates all national criminal intelligence, and that includes intelligence regarding paedophiles and crimes committed via the Internet. Further, the incorporation of the Australian Bureau of Criminal Intelligence, into the ACC has given the Commission responsibility for information and projects which concern child sex offenders.[1]

3.2 Three main areas of concern to the Inquiry emerged during the Committee hearings:

- access to the Internet and its use to transmit pornographic child sex imagery;
- the 'grooming' in chat rooms by paedophiles which can end in actual contact with the child; and
- ease of access to material unsuitable for children.

3.3 The dangers to children emanate from two areas: the active seeking out of children for chat room activity, and the availability of unsuitable material on the Internet for children to view.

3.4 Associated with this activity are the problems of investigation, detection, gathering evidence and prosecuting. The ephemeral nature of Internet material, and the absence of any requirement for Internet Service Providers (ISPs) to retain records, demands swift action before the evidence disappears. While there is a general discussion of these issues in Chapter 2, this chapter focuses on the impact on paedophile cyber activity.

The internet and anonymity

3.5 The evidence provided to the Committee demonstrated that the Internet has brought with it a global facility which allows paedophiles to extend their activities in a clandestine way. Reports of adults preying on children through the use of Internet 'chat rooms' have periodically featured on news bulletins, and were also referred to in the course of the Committee's hearings.[2]

---

1 *Committee Hansard* 18 July 2003, pp. 6 -7

2 e.g *Committee Hansard* 17 July 2003, pp. 30-31; *Committee Hansard* 18 July 2003, pp. 7-8; 16-20; *Committee Hansard* 21 July 2003, pp. 6-9.

3.6 The pace of technological progress allows more opportunities for paedophiles to use the Internet in more sophisticated ways. In his submission to the Inquiry, Mr Darren Brookes[3] noted that there has been significant change in the methods of operation of paedophiles in a short time. Mr Brookes gives the example of the development of the 'web cam' which allows live images to be broadcast to chat rooms and Internet computer conferencing (known as IRC or Internet Relay Chat).[4]

3.7 A submission from Mr Doug Stead, President of a Canadian Company 'Tri-M' related an example of an Australian on-line predator who was able to co-opt a Canadian child using relatively simple technology. The example also highlighted the co-operation between Australian and Canadian police in intercepting the perpetrator. [5]

3.8 The Australian Broadcasting Authority (ABA) also referred to the increased opportunities provided by the Internet for paedophile activity and noted that this has been a focus of concern for policy makers, the Internet industry and child welfare.[6]

3.9 In their submission to this inquiry, the National Child Protection Clearing House (which operates from the Institute of Family Studies) said:

> The Internet has become a popular means of recruiting children for sexual purposes because it provides easy access to children and a reduced risk to offenders of being identified.[7]

3.10 Similar concerns were expressed by the Victoria Police:

> Millions of child pornography images and movies are available on the Internet via news groups, peer to peer sites, chat channels ... A number of commercial organised rings have been identified and those sites have turned over many hundreds of thousands of dollars[8].

3.11 The Committee observed that the anonymity of this environment also allows the formation of web-based communities in which material can be exchanged by like-minded individuals.

3.12 In his submission to the Inquiry, Dr Patrick Forde from the Curtin Business School observed that email remailers (where there is an interim mail address which does not trace back to the initiating address) or hidden peer-to-peer networks are

---

3 Mr Brookes is a former lecturer at Goulburn Police Academy, and more recently was the Head of the Paedophile Unit (Interactive) in the United Kingdom. He is a Fulbright Scholar who is undertaking a PhD on the characteristics of Internet paedophilia at Washington State University.

4 Submission no 2, p.5

5 Submission no 3, pp.2-3

6 Submission. no 15, p.6

7 Submission no 7, p.3

8 *Committee Hansard,* 17 July 2003, p. 37

examples of advanced Internet devices which require considerable technical knowledge to use. (A peer-to-peer network is sometimes abbreviated to 'P2P'. It refers to any group of individual computers that can communicate with one another. Some of these operate undetected under the normal Internet structure, and are extensively used by paedophiles to distribute illegal and objectionable material.[9])

Pornographic imagery: Possession and Access

3.13 There is also the associated matter of unsolicited material sent by email and the extent to which its presence on a person's computer, even unopened, can constitute an offence of possession of pornography.

3.14 In its submission, Electronic Frontiers noted that:

> [Not only are] Internet users confronted with unwanted material, they also face the risk of criminal conviction for possession of material that came into their possession without their knowledge or consent. Generally, recipients of this type of material suffer in silence because if they report the criminal activity to law enforcement agencies, they risk being prosecuted for possession. [10]

3.15 In evidence, it was claimed that recipients of unwanted obscene e-mails who had reported them to the police were then charged with possession of pornography.[11]

3.16 The Committee noted that the situation outlined in this evidence has the potential to criminalise activity which may not deserve that description. The issue which arises from this is: when can an email be said to be in the possession of a person? There are several possibilities:

- when it lands in the computer mailbox;
- when it is opened by the addressee;
- when it is downloaded by the addressee and saved and printed.

3.17 The issue of the nature of possession of material on computers was a recurring one throughout the Inquiry.

3.18 The Committee observed that the law on this area varies from state to state, and there is no Commonwealth legislation which is specifically directed at this area. For example, in New South Wales, the offence of possession of child pornography (Section 578B *Crimes Act 1900 NSW*), is a summary offence, and the maximum penalty is 2 years imprisonment or 100 penalty units ($11,000).

---

9 Submission no 8, p. 1

10 Submission no 4, p. 3

11 *Committee Hansard,* 21 July 2003, p.59

3.19 In contrast, the Committee noted that under section 70 of the *Crimes Act 1958* (*Victoria*), the offence of 'knowingly possess child pornography', is indictable, and the maximum penalty is 5 years imprisonment, with no option of a fine.

3.20 There is currently no similar Commonwealth legislation with the exception of the *Classification (Publications, Films and Computer Games) Act 1995*, which is very limited in scope to those items unclassified or those classified RC (refused classification).

3.21 The nationwide (and worldwide) disparity in offence provisions, defences, and penalties is a barrier to effective control of this material. Furthermore, the jurisdictional issues raised by Internet material being circulated around the country and around the world make efficient detection of its source extremely difficult and resource intensive.

3.22 The Committee notes with concern that the lack of consistent legislation in this area is an impediment to detection and prevention of these offences. The differences in penalties, and in the nature of what constitutes an offence can result in activities which when perpetrated in one jurisdiction are a minor offence, but when committed in another jurisdiction are more serious. Without consistent approaches across jurisdictions the ability to eliminate this behaviour is weakened. While it is clear that there are significant jurisdictional issues involved in developing and implementing a nationally (and internationally) consistent system of offences and penalties, the Committee considers it a matter of urgency to ensure as far as possible that there are consistent sanctions and penalties applied to these offences across the country.

3.23 In this context the Committee notes the evidence from the Attorney-General's Department that:

> the government will introduce new offences and will provide a nationwide avenue to investigate, prosecute and punish those who use the Internet for trade in child pornography. These offences would carry a maximum penalty of 10 years imprisonment which [is similar to that which] would apply for bringing in hard copies through the customs barrier.[12]

3.24 The Attorney-General's Department indicated that the proposed legislative amendments will be released as an exposure draft. The Committee supports the release as an exposure draft and considers that it is important that the timelines for public discussion be sufficient for informed public consideration.

Use of chat rooms by children

3.25 Computer literate children can easily use the chat room environment. There is currently no way of effectively preventing Internet chat room activity engaged in by paedophiles and their victims. The Victoria Police noted in their submission that many

12 *Committee Hansard* , 21 July 2003, p.74

paedophiles adopt the on-line profile of a young child,[13] and 'groom' them for later meetings, all of which goes undetected.

3.26 In evidence the Australian High Tech Crime Centre (AHTCC) told the Committee that the Internet can include hundreds of thousands of potential offenders.[14] The nature of the offence makes control imperative but the size of the problem militates against effective detection and prevention.

3.27 The NSW Police told the hearing that the United States Federal Bureau of Investigation engages covertly in chat rooms to identify paedophiles.[15] There is no shortage of offenders, but the problem is determining who is the most dangerous, and who should be targeted first. The Committee notes that implied in this is a method of determining a profile of those most at risk as well as those who are most likely to offend.

3.28 Some guidance was offered by the National Child Protection Clearing House (NCPCH) who stated in their submission to the Inquiry that the ease of access and the anonymity of the Internet made it a perfect environment for a paedophile to misrepresent himself as another child or friend or a 'caring parent figure' to vulnerable children.

3.29 The NPC Clearing House cited some limited research from the U.S. which gives some indication of those who may be at risk as victims of Internet sexual offenders. The list of profiles includes:

- children with low self esteem;
- children who have been maltreated;
- immature children with learning or social problems;
- children over 14 who had been exposed to 'negative life events' (maltreatment or depression).[16]

3.30 The NPC Clearing House also indicated similar research has been done on the profile of typical offenders, and while urging caution, cited a UNESCO meeting of experts on child abuse and the Internet which noted a recent increase in offences by people who are sexually indiscriminate and who use children if they are available.[17] In evidence, the NPC Clearing House added that parents often do not realise the extent to which children access the Internet in multiple ways.[18] This suggests to the

---

13 Submission no 25, p.1

14 *Committee Hansard,* 21 July 2003, p. 16

15 *Committee Hansard,* 18 July 2003, p. 84

16 Submission no 7, pp.3-4, citing Finkelhor and Wolak 2001, Petraitis and O'Connor 1999, and Mitchell et al 2001.

17 Submission no 7, p. 4 also citing Arnaldo 2001

18 *Committee Hansard*, 17 July 2003, p. 32

Committee that the supervision of a child's computer use is an important factor in the prevention of child exploitation and abuse by Internet paedophiles.

3.31 The Committee notes that in the United Kingdom, the Government has acted on the use of chat rooms by paedophiles to target children. The ABA informed the Committee that the *Sexual Offences Bill* [HL] would make using a chat room or similar place for the purpose of engaging a child in paedophile activity a special offence.[19]

Access to unsuitable content by children

3.32 At its Melbourne hearing, the Committee observed that the availability of unsuitable material to children is an Internet access issue. At the Ninth Australasian Conference on Child Abuse and Neglect, held in Sydney on 24 to 27 November 2003 the potential risk of this access was illustrated in the paper entitled 'Child Protection and the Internet'. The authors noted disturbing research from the Canberra Hospital which:

> showed that sexually aggressive children under ten years, who have not personally experienced sexual assault but who have had exposure to sexually offensive material, are being seen at an unprecedented level. [20]

3.33 The Committee notes there is a dilemma in allowing adult access to material which should be restricted for children, but not necessarily for adults.[21]

3.34 The Committee looked at what is available for parents to monitor and control their children's use of the Internet. The ABA told the Inquiry of a number of initiatives which it has established to promote community awareness of Internet safety in Australia. They include:

- Publications for parents and children regarding the safe use of the Internet.
- Cooperative arrangements with a number of bodies, including educational authorities to distribute this material.
- A web site.
- The registration of Internet Codes of Practice.
- A complaints mechanism which can result in websites originating in Australia being removed, and those originating overseas to an international organisation. This only applies to websites, and not to chat rooms.

---

19 *Committee Hansard,* 18 July 2003, pp 15-16

20 Abstract of paper 'Child Protection and the Internet' presented by Dr Janet Stanley, Ms Cassandra Tinning and Ms Katie Kovacs at the Ninth Australasian Conference on Child Abuse and Neglect at website http://www.community.nsw.gov.au/accan/ viewed on 15 December 2003.

21 *Committee Hansard,* 17 July 2003, p. 30

3.35 The Committee was also informed about a number of filtering software packages, which can be installed on computers to block access to unsuitable material, and prevent unsuitable material reaching the user. The filters currently available do not block chat room activity.

3.36 There were reservations about the effectiveness of these programs. The ABA's pamphlets warn of the limited effectiveness of filters, and in evidence the ABA added that they are not the sole tool upon which parents should rely:

> [A filter] either shoots too wide or it is too narrow. It lets in material that it should not, and it stops material that you would not be offended by if your children saw it.[22]

3.37 This view was also held by Symantec Australia who told the Committee that:

> … you will never get 100 per cent risk reduction ... you will never be able to filter out all the pornography, the bomb-making recipes, the nasty pictures or anything that is used in chat rooms … The tools are not strong enough to be able to manage heuristics or artificial intelligence to the level that people would like to see.[23]

3.38 Symantec also took the view which was supported by other witnesses and submittors on this subject that there is no substitute for parental supervision of children's Internet use.[24]

3.39 The Committee also considers that while it is clear that Internet filtering devices can be of some use in supporting parents in their supervisory task, the evidence has demonstrated that solely to rely on these to prevent children seeing and having access to inappropriate material still risks exposing the children to that material, or inhibits adults' access to items which may be quite suitable for them, but not for their children.

3.40 The Committee observed that, while there are educational initiatives which publicise the dangers of children's unsupervised use of the Internet (such as those pursued by the ABA), they do not appear as yet to be as widely disseminated as they need to be in order to be effective. The Committee notes that such a public education role is not one that falls within the parameters of the ACC's functions. However, in this context the Committee is particularly mindful of the terms of The United Nations resolution no. 55/63: 'Combating the Criminal Misuse of the Information Technologies' which clearly states that the public should be made aware of the 'need

---

22 *Committee Hansard* , 18 July 2003, p. 21.

23 *Committee Hansard* , 18 July 2003, p. 76

24 For example, Submission nos 4, and 15; *Committee Hansard,* 18 July 2003, p.86.

to prevent and combat the criminal misuse of information technologies.' [25] (See Appendix 4).

3.41 While acknowledging that there are always financial constraints on providing published resources and advertising, the Committee believes that an awareness by parents of the potential criminal use of the Internet, and in particular chat rooms, in relation to children should be promoted. Equally, there is a need for parents to accept that they have a responsibility to supervise and monitor their children's use of the Internet. The evidence provided to the Committee supported the involvement of parents in their children's Internet usage, as a measure to prevent their exposure to unsuitable content.

3.42 The Committee is of the view that parents and children alike need the information. It commends the work the ABA is undertaking in this respect but that work needs to be reinforced. The Committee believes that reinforcing the ABA's message should take place across a number of media and should include a community service program.

Recommendation 2

The Committee recommends that the Government investigate partnerships for establishing a multimedia public education campaign on the risks associated with and the safe use of information technology by children, including parental supervision.

Investigating and detecting

3.43 The investigation of Internet paedophile activity is a challenge for law enforcement agencies and raises privacy issues which were of concern to some witnesses.

3.44 The Committee is aware that if inappropriate activity on the Internet which is designed to entrap children is to be a criminal offence, evidence must be obtained which will secure a conviction. The Committee heard that to obtain evidence of paedophile chat room activity, police need to have the capacity to monitor or intercept the person's Internet use.

3.45 There are several ways to undertake criminal investigations which involve the use of information technology. Searches can be conducted to check information stored on the user's hard drive but PricewaterhouseCoopers described a system which uses an Internet Service Provider's (ISP) log of those who have surfed the Internet through that particular ISP. It is possible to trace both the caller and the called.[26]

---

25 Resolution no. 55/63, paragraph (h), of the Un General Assembly, 81st Plenary Meeting 4 December 2000; http://ods-dds-ny.un.org/doc/UNDOC/GEN/N00/563/17

26 *Committee Hansard*, 21 July 2003, p.67

3.46 However, ISPs are not required to retain their logs for any period of time. Historically this was because of the expense and space required to store them; the cost has diminished, and it appears to be feasible to have ISPs retain records at least for a short time. While there is no legislative requirement on ISP to maintain records, there is a draft Code of Practice which seeks to establish a co-operative working relationship between the Internet industry and ISPs (see paragraphs 2.66 to 2.68).

3.47 The Committee heard that there is already a code of conduct for commercial television, and for Internet service providers. However, there was a view that self regulation may not be successful in protecting children effectively from undesirable contact and material. In a submission to the Inquiry, the National Child Protection Clearing House recommended:

> Internet Service Providers should be required to take greater responsibility for the protection of children by moving from self-regulation to quasi regulation or explicit government regulation, both of which are common in other industries in Australia.[27]

3.48 The submission also states that the (limited) number of websites explored in compiling the submission suggests that the Australian Internet Industry does not have a significant presence in addressing child protection issues.[28] One solution proposed was a system of ISP accreditation which would require certain levels of operating standards – such as the filtering of certain material.

3.49 In their submission to the Inquiry, Mr Julian and Ms Leanne Winch drew the Committee's attention to the availability in the United States of a free server-based filtering system, which customers can choose to activate as soon as they sign on to the service. The submission notes that some service providers do offer this option but recommends that free optional server-based filters should be available, and service providers who fail to offer the filter should be heavily fined.[29]

3.50 Under the current arrangements, the Committee is concerned that it appears that self regulation by the Industry in this area may not be adequate. The Committee is of the view that honouring the terms of the Code of Practice requires both an acceptance of the code and the resources to discharge the requirements. The Committee received a copy of it during the Inquiry. However, it did not receive any evidence from ISPs. This was despite attempts by the Committee to speak with some ISPs operating within Australia. The Committee therefore must question the level of acceptance of the code within the industry.

3.51 Notwithstanding the industry's ability to comply with Law Enforcement Agencies' (LEA) requests for records there can be little argument that the collection

---

27 Submission no 7, p.1

28 Submission no 7, p 9

29 Submission no 31, p.1

of such evidence is critical to prosecution. While it also presents a useful avenue for detection, the records are not the only avenue.

3.52 The AHTCC told the Committee of some of the strategies used abroad. Federal Agent MacGibbon told the Inquiry that an officer from the AHTCC had been examining procedures in the UK and the US:

> The Internet means that you have hundreds of thousands of potential offenders in these chat rooms, and you need to know how to filter it down to a reasonable number so that you can have the level of suspicion or belief about it that lets you do the extra, more intrusive investigative aspects — how you locate that offender and how you look at engaging them in the physical world …
>
> … the [Innocent Images Program is the] FBI's main child sex investigations area and which also maintains a proactive online presence, posing as children online and engaging people in conversation. [30]

3.53 The Committee notes from the AHTCC's evidence that it is allocating a high priority both to the legislative and forensic aspects of this criminal activity.[31]

3.54 The NSW Police told the Committee that the American FBI engages covertly in chat room activity in order to track paedophiles. However, the American experience has been that there is such a proliferation of paedophile activity in chat rooms, that the agents have to select which offenders they will target.[32]

3.55 In evidence, Mr Gregory Melick observed that:

> To randomly try to pluck something out of the ether and interpret it to see what is going on will be almost impossible. You also have the other problems of encryption and steganography.[33]

3.56 The US experience and Mr Melick's comments suggest that any requirements placed on ISPs to provide records should be targeted with some knowledge of illegal behaviour rather than a global search the ISP records. The responsibility placed on ISPs is therefore reduced and the resource requirements in searching the material seized is also limited.

3.57 Any seizure of the users' hard drives for evidentiary data could also be obtained in the context of pre-existing knowledge. For law enforcement agencies to direct a more 'intrusive investigation' to a wide spectrum of users would be a costly exercise with a doubtful return.

---

30 *Committee Hansard*, 21 July 2003, p.16

31 *Committee Hansard*, 21 July 2003, p.16 -17

32 *Committee Hansard*, 18 July 2003, p. 84-85

33 *Committee Hansard,* 21 July 2003, p. 32

3.58 The Committee notes that seizure of suspect computer hard drives and associated records is already available under Commonwealth and State search warrant legislation.

3.59 The NSW Police suggested the following possible legislative changes to assist in the detection and prosecution of paedophiles: [34]

- amendments to the telephone intercept legislation to include child pornography and enticement;
- amendments to NSW legislation concerning possession and publication of child pornography, and
- a new offence (similar to that being contemplated in Britain and discussed in paragraph 3.31), of online grooming and luring for the purpose of a sexual act.

3.60 The Committee notes that the last of these initiatives in particular has considerable potential for affecting online chat room activity. However, the problem of Internet paedophilia is an interstate and national one, as is cybercrime generally, and the legislative solutions to be most effective must be nationally consistent and if possible, internationally.

3.61 Further, there was some concern that to extend the LEAs' powers to intercept and seize in any way would raise issues of civil liberties and rights to privacy which currently exist. The ACC itself acknowledged this in evidence.[35]

3.62 In their submission Electronic Frontiers Australia indicated that any proposal which would increase powers for law enforcement agencies should be carefully scrutinised. EFA noted that there are already provisions (under the *Telecommunications Act 1997)* which allow some law enforcement agencies to make certified and uncertified requests to a carrier or carriage service provider for disclosure about telecommunications users.[36] EFA considers that any extension of these powers would not be justified in the absence of evidence that the measures would have the intended impact on criminal activity.

3.63 The Committee did not form the view that an increase in the interception powers of law enforcement agencies to investigate paedophile activity on the Internet was warranted but it was concerned that there still is no uniform legislation governing the collection and use of evidence. The Commonwealth *Evidence Act 1995* was intended to be adopted co-operatively by all states and territories; however the Commonwealth Act applies only to Commonwealth investigations, and has been adopted as far as possible in New South Wales and applied to State investigations. The Committee was advised that Victoria is examining the proposal.[37] However, the

---

34 Submission no 17, p.2

35 *Committee Hansard,* 18 July 2003, p.5

36 Submission 4, p.10

37 *Committee Hansard*, 17 July 2003, p.17

Committee notes that a report was prepared for the Victorian Parliament in 1996 recommending adoption of the Commonwealth and NSW Evidence Act models[38] and it is yet to be implemented.

Recommendation 3

The Committee recommends that the Commonwealth Attorney-General liaises with the State and Territory Attorneys-General to ensure that priority is given to the development and implementation of consistent offence and evidence legislation in relation to cybercrime, which is in accordance with Australia's international obligations.

3.64 The Committee was advised that there are proposals for legislation at Commonwealth level. [39] It considers that, given the international experience of the proliferation of predatory paedophile behaviour using information technology, the new offence relating to 'online grooming' and luring of children for the purpose of a sexual act (proposed in the British legislation) would be a useful addition to the statute books in Australia.

Recommendation 4

The Committee recommends that as part of its legislative package to detect and prosecute those who use information technology for the trade of child pornography, the Government introduce a new offence relating to luring and grooming children for sexual purposes.

3.65 Finally, the Committee notes the suggestion by PricewaterhouseCoopers relating to a keystroke logger. This logger can record every single keystroke, and thus trace the Internet activity of the user. However, the legality of this device has yet to be tested and the Committee suggests that the matter warrants further examination.

National register of child sex offenders

3.66 It is clear to the Committee that in the light of the expense involved in this area of investigation, that resources need to be focused where they will obtain the most effective results. The Committee heard that one way this could occur would be in cases:

> involving the prosecution of individuals who may have attracted the attention of law enforcement for other, perhaps unrelated reasons. In the course of investigation the evidence of other illicit materials has been found

38 Report of the Scrutiny of Acts and Regulations Committee, Parliament of Victoria, 'Review of the Evidence Act' 1996.

39 Attorney General's Department, Submission no 21 and *Committee Hansard,* 21 July 2003, pp 73ff.

> on their computer, perhaps leading to a trail of other offenders with whom that other individual may have been in contact.[40]

3.67 The Committee considers that a national register of Child Sex Offenders would be useful in this process. The Committee is aware that the NSW Government has a database of child sex offenders which includes their names, addresses, employment and car registration details. The register is not public but is available to law enforcement agencies. Recently a meeting of Australian Police Ministers agreed to the establishment of a similar national database. The register will also allow Australia to endorse international child protection agreements.

3.68 The Committee was aware that the development of a national database could result in a number of situations having the potential for unintended consequences: for example, where somebody appears on the register because they were convicted under age of consent laws, rather than arguably more serious, and/or aggravated sex offences.[41] However, the Committee, having discussed the matter with officers from the Attorney-General's Department, is confident that sufficient safeguards and redress would be included in any such register, particularly for those who might find themselves in that position.[42]

Conclusion

The Committee notes that in relation to paedophiles, and children's access to unsuitable material on the Internet there are initiatives which focus on prevention and protection. The international experience suggests that information technology has been readily adopted by those who are involved in both the purveying of child pornography and the pursuit of children for sexual purposes. To assist in the detection and prosecution of these offences in Australia, the Committee has made a number of recommendations in relation to this aspect of the inquiry. However, the Committee believes that the most significant role for the ACC is in intelligence collection; the problem is, by its nature, international and subject to the vagaries and priorities of the law of other jurisdictions.

---

40 *Committee Hansard*, 21 July 2003, p.2

41 *Committee Hansard*, 21 July 2003, p.81

42 *Committee Hansard,* 21 July 2003, p.81

Chapter 4

Banking, Credit Card Fraud and Money Laundering

The banking industry

4.1 Most Australian consumers are affected in one way or another by electronic banking. The banks use their cyberspace networks to process transactions, and to communicate with the many clients who have taken up Internet banking. The potential for cyberfraud covers a number of banking areas. They include Internet banking, credit and debit card fraud, money laundering and related offences such as identity theft and securities and investment fraud.

4.2 The Australian Bankers' Association (the ABksA) appeared before the Inquiry and also provided a submission. In the introduction to its submission the ABksA indicated its position on the subject of the Inquiry:[1]

- The current regulatory framework covering cybercrime is satisfactory and no further legislation or regulation is required at the Commonwealth level.
- Customers have a vital role to play in protecting their own interests, and banks will continue to provide financial literacy programs including cybercrime self-protection.
- State and Federal Governments also have a vital role to play in providing education programs to ensure customers better understand their responsibilities in protecting their own interests.
- The banking industry is a vital component of the critical infrastructure that underpins the whole of the Australian economy and Government should assist banks and other stakeholders in protecting this national asset.

4.3 The Committee notes the banks' emphasis on consumer responsibility for self protection from fraud, rather than the banks' duty to protect their customers. This emerged as a significant issue during the course of the Inquiry. The Committee notes that both consumers and banks have a number of options at their disposal to increase fraud protection. This chapter notes the most significant of those options.

Internet banking

4.4 Internet banking allows bank customers to view statements online, pay bills, transfer funds between accounts, make inquiries, order cheque books, and to do almost anything which can be done at the bank itself, except withdraw cash!

---

1 Australian Bankers' Association, Submission no.19, p.5

4.5 Internet banking is subject to all the same financial transaction reporting, proceeds of crime and taxation laws as other banking services.[2]

4.6 Banks have been enthusiastic in their encouragement of clients to adopt Internet banking as noted in the ABksA submission:

> Banks have embarked on the development and deployment of Internet banking facilities because the market has demanded that banks provide a secure and trusted environment for the delivery of a wide range of financial services in a convenient and cost effective manner. [3]

4.7 The development of e-banking, and its acceptance by society has seen the emergence of new ways to perpetrate 'old' crimes such as fraud and money laundering and the development of new crimes. These crimes are using and at times taking advantage of the same technology as e-banking.

4.8 The evidence presented to the Committee revealed different ways of manipulating the Internet banking environment. Apart from the Nigerian email letters in which criminals set up false 'authentic' accounts to receive the transferred money, there have been bogus bank sites established which then request 'confirmation' of account details – such as passwords and account numbers. The Committee heard that it is not difficult to duplicate features such as the logo of the bank, and the layout of the website, all of which is designed to deceive the bank customer.[4]

4.9 In evidence, the Australian Bankers' Association noted that the banks in the bogus bank example were able to respond with the assistance of the Australian Federal Police[5] within hours and the sites were shut down. The banks also emphasised in the ensuing publicity that banks never request 'verification' of details through the Internet, and that passwords should be revealed to no-one.

4.10 The Committee notes the comments of ASIC who acknowledged the role of Internet technologies in providing new opportunities for people to engage in new types of scams such as the email referred to above. ASIC said in evidence:

> … Without spam and Internet technology, that crime would not occur. The fact that we have seen reported in the press something like half a dozen of those matters in the last three or four months does not necessarily equate to a flood. To balance that up, … they very quickly were able to identify the Australian connection, they worked with the New South Wales Police, and someone was arrested within three days of that spam email going out. I understand that person has been charged subsequently with deception. … it

2 Submission no. 23, p. 23

3 Submission no. 19, p.19

4 *Committee Hansard*, 18 July 2003, p. 44

5 *Committee Hansard*, 18 July 2003, p. 44

> appears that the financial institutions, working with the police services, are able to protect themselves adequately and take recourse.[6]

Prevention – Internet banking security

4.11 The Committee notes that the ABksA indicates that banks are addressing prevention and detection of criminal activity in banking and credit card transactions through a number of avenues. [7]

4.12 In relation to the issue of prevention, the Committee received evidence which revealed some concerns regarding the security of Internet banking. A submission from Mr Tony Healy[8] expressed concern that banks do not use strategies which can assist with the prevention of Internet banking fraud.

4.13 Mr Healy notes that traditionally, retrieval of funds from an account required the presentation of a physical token (passbook or ATM card) combined with secret information (PIN or personal signature).

4.14 When Internet banking commenced, the second element was provided through digital certificates, given to each client and installed on the client's computer. However, these were expensive, and banks moved to the cheaper option of password protection only. Mr Healy considers this is weak protection, as passwords can be obtained through the activity of viruses or through being stored on the browser, and thus being available to any user of that computer.

4.15 Finally, Mr Healy notes that the customer is responsible for the security of the password, and under most electronic banking contracts, its revelation even if not by the client, constitutes negligence.

4.16 Mr Healy was not alone in his disquiet. In evidence to the Committee Mr Steve Orlowski said that in the current banking environment the standard of Internet banking security is 'just' adequate,[9] and most of the problems occurring at the moment are due to inadequacy of the banks' protective anti-hijacking measures. Mr Orlowski continued:

> The Internet itself is not the problem; it is what is happening at the end point where the data is being held.[10]

4.17 The Committee was concerned, that despite the banks' confidence in their security, there are clearly significant data protection issues which concern the experts

---

6 *Committee Hansard,* 21 July 2003 p. 47

7 Submission No. 19, pp. 13-14

8 Submission no. 14, p. 2

9 *Committee Hansard*, 17 July 2003, p. 7. Mr Orlowski is a private consultant and is also the chair of APEC's eSecurity Task Group.

10 *Committee Hansard*, 17 July 2003, ibid.

in the area. Mr Orlowski noted that the banks are moving towards stronger protection and will be implementing an electronic authentication system. This is expected to provide a much stronger access control technique for users.

4.18 The Committee considers that part of the solution is to use public education campaigns to prevent customers from being defrauded by fictitious websites. However the Committee does not accept the assertion of the banks that this is solely the role of government; it is clearly part of the banks' client service role, to provide information to its customers, which as far as possible ensures that they deal with the bank itself.

4.19 In evidence ASIC noted that its interest is very much from the consumer protection angle. ASIC ensures that financial institutions are aware of the threats, that they implement appropriate risk management strategies, provide clear instructions to their clients about their obligations and liabilities, as well as educating them about safe practices.

> Having said that, there is no doubt that the arrival of the Internet technologies of the Internet technologies has provided new opportunities for people to commit new types of scams … [In] one of those matters involving a large Australian financial institution … they very quickly were able to identify the Australian connection, … and someone was arrested within three days of that spam email going out.[11]

4.20 While noting ASIC's comment and the fact that there was a rapid response to the attempted fraud, it is only a matter of time before other ways of breaking into banking records are devised. In the Committee's view there is no room for complacency. The Australian Crime Commission (ACC) in conjunction with the Australian High Tech Crime Centre (AHTCC) are in a position through their intelligence activities to provide general information about fraud trends to financial institutions. This information could be provided through a third party which could collect and disseminate all available information on a regular basis.

Recommendation 5

The Committee recommends that the Australian Crime Commission in conjunction with the Australian High Tech Crime Centre investigate the provision of general information on fraud trends to financial institutions through a secure subscription based service.

Credit and debit card fraud

4.21 The introduction of the Bankcard to Australia by nine Australian banks in 1974, commenced a revolution in consumer purchasing. While some stores had offered credit cards and store based finance for many years, the concept of a

11 *Committee Hansard,* 21 July 2003, p. 48

universal credit card administered by the banks allowed bank-funded credit to be extended to new areas of consumer activity.

4.22 With the credit card purchasing power came the potential for large scale fraud. Advancing technology changed only the method of committing the fraud and has also required technological expertise used to investigate and detect fraud to advance.

4.23 Card Skimming involves a small device which will capture the card details for use in a reproduced card. In its submission to the Committee, the ACC noted that it is not only credit cards which can be skimmed for their information. These devices are also used at Automatic Teller Machines (ATMs) and card skimming can be used to obtain personal information from debit cards, and even Medicare cards. Over the past 12 months, credit card skimming alone has increased bank losses by 400 percent, and its actual cost to the banking industry, businesses and consumers is more than $300 million per year.[12]

4.24 In evidence, the NSW Police advised that a Fraud Squad task force had found that one of the main areas of card fraud is 'points of common purchase'.[13]

> A common purchase point is an area, usually a service station, where someone skims a user's card. The information is then passed on to criminal syndicates who reproduce cards en masse and on-sell them again … Service stations are about 75 per cent of the common purchase points.

4.25 The Committee was also informed in the ACC submission that card skimming is being perpetrated by organised crime groups:

> in conjunction with other serious cross jurisdictional and transnational criminal activities including drug trafficking, money laundering and potentially arms trafficking.[14]

4.26 The ACC also notes 'the social implications of card skimming are serious'.[15] Apart from the cost to banks, the victims are left with debts in their name for which they are held responsible unless and until the victim can show otherwise. The Commission continued:

> the rising incidence of credit card skimming is leading to the introduction of new controls that would shift the onus of harm from the financial sector to individuals. Such countermeasures are likely to impact adversely upon individuals.

---

12 Submission no. 23, p. 25

13 *Committee Hansard,* 18 July 2003, p. 87

14 Submission no. 23, p.30

15 Submission no. 23, p 27

4.27 The Committee shares the concerns of the ACC. The social and financial cost of forcing consumers to pay for harm resulting from credit card fraud is potentially high.

Merchants and credit cards

4.28 The Committee also heard from Mr Graeme Bond, a merchant who has had an ongoing disagreement with his bank since 1996, regarding a series of fraudulent credit transactions for which the bank has held him responsible. The Committee notes that Mr Bond's experience is more about a fraud which was perpetrated by means of a credit card, and the arrangements with his bank, than an Internet transaction. Mr Bond's experience illustrates the nature of the liability imposed through the agreements between banks and merchants.[16]

Prevention – Credit Card Skimming and Fraud

4.29 The ACC advised the Committee that credit card skimming has been approved by the ACC's Board as an approved intelligence investigation. Thus far, the activity has consisted of consultation with:

- New South Wales Police about their Task Force Venlo, which investigated credit card skimming in New South Wales;
- Discussing with the (credit) card companies risks and trends and what they believe law enforcement should be looking at in relation to card skimming.
- Participation in the MasterCard fraud reduction task force meeting.[17]

4.30 The ACC also noted that the card skimming appeared to have 'migrated' from South East Asia. The Committee observed that as the reference is quite recent, the ACC is still in the early stages of developing strategies. The ACC did advise the Committee that the AFP liaison network was doing some work in this area.[18]

4.31 The Committee was also told of a system of random checks to validate credit transactions which the banks undertake each day. In particular, if there are any unusual features of a transaction, the card holder will be contacted to check it was made by the card owner. The Committee was told that there are over 300 such calls made each day, and that the banks wear significant losses for the transactions fraudulently made.[19]

4.32 The Attorney General's Department pointed out that a number of peak bodies are developing ways in which card skimming can be eliminated. These include the Standing Committee of Attorneys General, the Australian Police

16 Submission No. 16

17 *Committee Hansard* , 18 July 2003, p.11

18 *Committee Hansard* , 18 July 2003, p.11

19 *Committee Hansard* , 18 July 2003, p.11

Ministers' Council, the Australian Bankers' Association, and a Commonwealth NSW task force.

4.33 However the banks do have other technology available. The so-called 'smart card' is a far more secure option than the magnetic stripe technology in current use.

> A smart card is made of plastic, and in size and appearance is similar to a normal credit card. [The card has a] microchip embedded in it … which replaces the magnetic stripe commonly found on the back of other transaction cards. [It] allows the storage and management of large amounts of different types of information. Most importantly, the microchip may allow the performance of computing tasks through a microprocessor included in the chip. Using the integrated circuit's memory capacity and processing power, one card can accommodate multiple applications providing greater flexibility and ease of use for the customer.[20]

4.34 The technology is used in security applications, and is difficult to replicate. It is expensive to produce, but is far more secure than its alternatives, and may represent a saving for financial institutions in the long term.

4.35 The Committee observes that banks and the promoters of credit cards derive considerable income benefits from their use by consumers and merchants; the cards are strongly promoted in many contexts. An example is the special sporting events cards, promoted and used initially at times when there are many itinerant people in one place, who are being encouraged to spend. The potential for fraudulent use in such circumstances represents an increased risk. Where the card holder can be shown to have been reckless in the care and storage of the card and its details, it is clear where the liability for misuse lies. In cases where neither the financial institution nor the cardholder has compromised security, there is clearly an increased cost to the bank which should not be borne entirely by either the bank or the client cardholder.

4.36 However, in cases where neither the financial institution nor the card holder has been negligent, the allocation of liability is not nearly so clear. The approaches currently available to resolve this issue were developed in pre-electronic banking, pre-Internet times. The Committee is of the view that given the increased potential for fraudulent use in the e-environment, the issue warrants an approach which is grounded in the electronic transmission of documents, rather than their physical presentation.

Identity fraud

4.37 Closely associated with banking and credit card fraud is identity fraud. The Victoria Police told the Committee hearing that identity related crimes are evident in most fraud related offences, including loan applications, credit card fraud and online

20 http://www.smartcardforum.asn.au/smartcard.htm

banking. Globally, this activity is currently one of law enforcement's greatest problems.[21]

4.38 The ACC noted in its evidence that identity fraud is used as a means to commit drug, firearms and e-crime offences.[22] Identity fraud offers opportunists and those who shift from one area to another an easy way to pursue the quickest way of making money, whether it is by drugs, guns, prostitution or white-collar crime.

4.39 In this context, one of the issues which arose was the integrity of the 100 point check, used by banks to establish the identity of a person wishing to open an account. The system is established under the *Financial Transaction Reports Act 1988.* As AUSTRAC pointed out in evidence, the documentation was not created with the identification system in mind:

> Birth certificates, passports, drivers' licences and even credit cards – all these sorts of things – can be used as part of the process. The system is okay; it is the integrity of the documents and the ability to verify them that creates the difficulty in the process.[23]

4.40 The ABksA advised the Committee that new technologies such as scanners, and colour printers have increased the banks' exposure to identity fraud, and that it is relatively easy to produce false documents of high quality.[24]

4.41 The Committee notes that while the 100 point check in itself is clearly a useful tool – 'a robust identification system' – the issue is increasingly the underlying integrity of the documents.[25]

4.42 In evidence, AUSTRAC told the Inquiry of a Proof of Identity Committee chaired by AUSTRAC which is examining some of the options which might be available to verify claims to identity.[26] AUSTRAC suggested that a system of fast-track verification of documents would be of benefit and also suggested the possibility of a facial and iris recognition system known as biometrics.

4.43 This was also raised by Standards Australia which has developed a number of standards for the use of information technology in the banking system, for example, the maintenance of security for the operation of ATMs.[27]

---

21 *Committee Hansard*, 17 July 2003, p. 37

22 *Committee Hansard*, 18 July 2003, p. 11

23 *Committee Hansard*, 18 July 2003, p. 64

24 *Committee Hansard*, 18 July 2003, p. 45

25 *Committee Hansard,* 18 July 2003, p. 64

26 *Committee Hansard*, 18 July 2003, p. 63

27 *Committee Hansard*, 18 July 2003, p. 52

4.44 Biometrics is the identification of people through face recognition, fingerprints, iris recognition, retina recognition (visual recognition), auditory (voice) recognition and also includes chemical, behavioural and olfactory analysis.[28] It is already being used by private firms to verify identities. As with any identification procedure privacy is an issue and Standards Australia advised that Codes of Ethics are being development by the Biometrics Institute for this purpose.[29]

4.45 The Attorney General's Department told the Committee that the Criminal Code includes specific fraud offences.[30] Identity fraud is a feature of welfare and tax fraud offences, along with increasingly being featured in organised crime. The Department also advised that it is developing a strategic direction for improved personal identification and authentication practices. For example, the AUSTRAC Proof of Identity Steering Committee is assessing the community cost of identity fraud. The steering committee includes representatives from the banking industry as well as government agencies.

4.46 In addition, the ACC has maintained the Identity Fraud Register which lists known offenders, fraudulent names used and lost or stolen documents. The Australian Bureau of Criminal Intelligence (ABCI) established this project in 2001, and the ACC submission indicates that over 2000 recent fraudulent identities have been recorded on the database. The database can link offenders with real identities and crimes and is designed to facilitate the work of law enforcement agencies (LEAs).[31] The Committee commends this initiative.

4.47 The Committee encourages the continuation of the close working relationship between the banks and the police – both state and federal.[32] Cross sector liaison is essential for the sharing of information and the development of strategies to minimise the effect of cybercrime.

4.48 However, as was indicated in the evidence provided by Symantec, the implementation of strategies and technology depends upon the cost of the technology and persuading people to use it.

> … you have to make this cost-benefit analysis and if the financial institutions in a particular country have decided that there is an acceptable level of risk with a technology they are using, they are going to continue with that technology.[33]

---

28 http://www.biometricsinstitute.org/bi/types.htm

29 *Committee Hansard,* 18 July 2003, p. 53

30 Submission no. 21, p.13

31 Submission no. 23, p.24

32 *Committee Hansard*, 18 July 2003, p. 43

33 *Committee Hansard*, 18 July 2003, p. 80

4.49 The Committee is disturbed at the notion of 'an acceptable level of risk' for the financial institutions. What is acceptable to the banks may not be acceptable to the consumers of the financial services provided. Where such an acceptable level has been determined, the consumers should at least be made aware of it and advised as to what they can do to minimise that risk.

Money laundering

4.50 Money laundering is defined by the OECD as:

> The processing of … criminal proceeds to disguise their illegal origin. This process is of critical importance, as it enables the criminal to enjoy these profits without jeopardising their source.[34]

4.51 In evidence the Committee heard that the OECD's associated Financial Action Task Force is an intergovernmental initiative whose purpose is the development and promotion of policies, both at national and international levels, to combat money laundering and terrorist financing.

4.52 The ACC advised the Committee that money laundering is one of the areas in which the Commission is authorised by the Board to use its coercive powers, along with associated criminal activities of South-East Asian crime gangs, established criminal networks and illegal firearms.[35]

4.53 The Australian Bankers' Association told the Committee of its very strong relationship with AUSTRAC. The banks, under the *Financial Transactions Reports Act 1988*, are required to report suspicious transactions to AUSTRAC, and the Association indicated that in addition to matters arising from traditional crime and money laundering, there is now also a focus on the suppression of the financing of terrorists.[36]

4.54 AUSTRAC's evidence noted its role as an observer and reporter on international funds transfer instructions or international telegraphic transfers. The agency has been turning its attention to what happens outside of the regulated financial markets, and the potential for the expansion of unregulated financial transactions.[37]

4.55 AUSTRAC advised the Inquiry that the AGEC (Action Group into the Law Enforcement Implications of Electronic Commerce) which is chaired by AUSTRAC, has also been examining this area in two of its focus groups: one on new technologies and the other on the financial system. The Group's membership includes the Australian Taxation Office, the Australian Federal Police, the

---

34 OECD website http://www1.oecd.org/fatf/MLaundering

35 *Committee Hansard,* 18 July 2003, p. 6

36 *Committee Hansard*, 18 July 2003, p. 36

37 *Committee Hansard*, 18 July 2003, p. 55

Commonwealth Attorney-General's Department, the Australian Competition and Consumer Commission, the Australian Securities and Investments Commission, the Australian Customs Service, the Director of Public Prosecutions, the Department of Immigration, Multicultural and Indigenous Affairs, and the Australian Prudential Regulation Authority.

4.56 AUSTRAC explained:

> [The AGEC is] looking at ways of avoiding the financial system … E-gold and other similar types of mechanisms have been of great interest, particularly to the Australian Taxation Office. People use them to avoid our reporting mechanisms … on international funds transactions. It is quite easy to use these mechanisms by buying e-gold and then having credit cards or debit cards on international accounts so that our reporting systems are completely avoided. There is quite a large amount of concern within the broader law enforcement agencies, including revenue and regulatory agencies, about those sorts of mechanisms.[38]

4.57 The Committee learned that such systems are simple to use, and can effectively transfer large sums undetected to and from Australian–owned 'accounts'.

Prevention – Money Laundering

4.58 In addition to the establishment of the AGEC Committee, the Committee was advised of other technical and strategic resources available to deal with money laundering.

4.59 The Attorney General's Department told the Committee that there are strategies available to combat money laundering. The threat of terrorism has given money laundering a new global focus apart from its traditional connection with organised crime.[39]

4.60 The Department also informed the Committee that Australia is a member of the international Financial Action Task Force on Money Laundering (the FATF), which has developed the Forty Recommendations – the basis of international anti-money laundering standards, which include sanctions against non-compliant countries.

4.61 Post 11 September 2001, the FATF released eight Special Recommendations on Terrorist Financing, accompanying the United Nations measures. A review of the Forty Recommendations is currently under way.

4.62 In 1997, the Asia Pacific Group on Money Laundering (APG) was established as a FATF-style regional body of 26 member states. The APG plays a

---

38 *Committee Hansard*, 18 July 2003, p. 58

39 Submission no 21, p.13

coordinating role in the provision of technical legal and law enforcement experts to countries in the region.

4.63 In addition to the *Financial Transactions Reports Act 1988,* money laundering, in the domestic arena, is managed within the framework of the *Proceeds of Crime Act 2002*. Under this legislation courts can freeze and confiscate assets under certain circumstances.

4.64 There is also state-based proceeds of crime legislation, which allow civil forfeiture of assets, in state offences. The ACC has frequently used this legislation to recover proceeds of crime, and under the Commonwealth legislation is in a position to assess the effectiveness of the *Proceeds of Crime Act 2002* in recovering laundered funds, and whether it is at all useful in recovering funds which have been transferred outside the reporting system.

Future directions for banking, credit card fraud and money laundering

Australia a vulnerable target

4.65 The ACC submission notes that there are limitations in the Australian national law enforcement's response to card skimming which can be exploited by being open to criminal activity. Further, the ACC considers that the increasing controls over card skimming activity in North America, Europe and Asia, and the lax legislative (multi-jurisdictional in one country), and deterrent environment is likely to result in transnational criminal groups shifting their activities to Australia.[40]

4.66 The ACC notes[41] a report in September 2002, by the Office of Strategic Criminal Assessments[42] (OSCA – now incorporated into the Australian Crime Commission) which predicted that the threat of card skimming would continue to rise, and cited a number of contributing factors. These included legislative gaps such as restrictions on the import of skimming equipment such as card blanks and skimmers; lack of jurisdictional agreement on what constitutes an offence, and lack of deterrence factors in criminal penalties.

4.67 OSCA also cited:

- systemic weaknesses in banking practice (such as lax merchant practices);
- lack of consumer awareness of card security;
- a gap in Australian law enforcement intelligence holdings; and
- an acknowledged need for a national intelligence gathering strategy.

---

40 Submission no 23, pp.27-28

41 Submission no 23, p.30

42 OSCA, *Fraud – Credit Card Skimming,* No. 02/02 September 2002

4.68 In the Committee's view, the ACC can make a significant contribution to the gap in intelligence holdings and the development of a national intelligence gathering strategy. OSCA, as part of the ACC is in a position to provide information on cyber fraud and related activity to law enforcement and policy bodies on a regular basis. The Committee notes that one of the strategies that the ACC identified as contributing to a national response included the provision of a national intelligence database on card skimming for enhanced intelligence exchange. It notes that this role would fill a gap in current law enforcement arrangements on card skimming.[43]

4.69 The Committee is of the view that this role should be expanded. During the Inquiry, it formed the view that there was the potential for inter-relationships between the various forms of banking cybercrime and that this potential should be explored.

Recommendation 6

The Committee recommends that the Australian Crime Centre, in consultation with the Australian High Tech Crime Centre (AHTCC), Austrac and other law enforcement agencies give priority to developing a national intelligence gathering strategy for cybercrime in the banking industry. Further the ACC should seek to fill any gaps in intelligence holdings that are identified.

4.70 In relation to consumer awareness of card security, the Committee notes that the ABksA considers that the Government has a role in public education programs to ensure that customers understand their responsibilities. Given the significance of banking in a community's economic health, the Committee believes it is necessary for government and financial institutions to form partnerships to support increased client awareness of the potential pitfalls.

4.71 The issue of the systemic weakness in banking practice may be overcome in part by education campaigns. The Committee notes that that the AHTCC advised that in May 2003, the AFP, AusCERT and other law enforcement agencies produced the *Australian computer crime and security survey*.[44] The AHTCC indicated the survey showed that:

- corporations are spending more money on IT security aspects; but also
- there are certain generic vulnerabilities within some industries.

4.72 These vulnerabilities demonstrate that there is a need for firewalls, intrusion detection systems and policies to prevent contamination from disks imported from outside an organisation's system.

4.73 In addition the AHTCC, Standards Australia and the Attorney-General's Department, have funded the production of a computer forensics guide for industry.

---

43 Submission No. 23, p. 32

44 *Committee Hansard*, 21 July 2003, p. 22

This is an evidence collection guide designed to advise the industry on how they may start protecting themselves gathering together the information that is needed to prosecute these matters effectively.

4.74 In his evidence to the Committee, Mr Orlowski referred to a number of potential solutions for protecting identity, and thereby eliminating some of the aspects of banking and credit card fraud. These include public key technology:

> which is a very strong security tool based on cryptography and which is seen as the cornerstone for electronic commerce in providing secure and authenticated electronic transactions.[45]

4.75 There is also the strengthening of technology through the use of smart cards which would mean that a person wanting access to another's data would require the card to do it, as it would be 'computationally infeasible' to break the information.[46]

4.76 Other technology which has potential in this area is biometrics (discussed in detail at paragraph 4.43). However, the NSW Police pointed out to the Committee that biometrics – for example, biometric links to credit data – as a security solution are really a matter of what the community will tolerate.[47] The Committee is aware of the sensitivity surrounding centralised access to personal data, and that there are compromises to be made if biometrics becomes the technology of choice.

4.77 The NSW Police also noted the overseas experience in which telephone lines are physically intercepted to pick up data. If at any point along the communication lines the data is not encrypted it has the potential to expose millions of users to capture or corruption of data.

4.78 The implications of failure to secure data are widespread. Not only could financial details be captured, but other personal and corporate material taken and used. The detection is difficult and resource intensive and there is also potential for civil litigation for those who suffer loss through no fault of their own. While it is a Commonwealth offence to intercept telecommunications without a warrant, there would also be offences arising out of the corruption or use of the data for gain or benefit. It is clear that law enforcement agencies should devise prevention and response strategies, in the event that telephone line intercepts occur in Australia. In particular, the ACC in partnership with the AHTCC is in a position to develop response strategies, based on its operational experience.

4.79 The Committee notes that in relation to credit card fraud, and in particular card skimming, the ACC considers that it has a role: its submission to the Inquiry indicates:

---

45 *Committee Hansard* , 17 July 2003, p. 2

46 *Committee Hansard*, 17 July 2003, p. 8

47 *Committee Hansard*, 18 July 2003, p. 88

> Although many of the specific offences associated with card skimming are fraud under State Criminal Codes, card skimming is appropriately regarded as federally relevant criminal activity and will require priority attention from national law enforcement.[48]

4.80 The ACC also advises that its contribution to a national response to this problem could include a series of strategies:

- focusing on the multi-jurisdictional and national dimensions of card skimming;
- utilising specialist financial investigation resources to complement the expertise of partner agencies;
- using cybercrime investigation methods and forensic techniques;
- providing enhanced insight into the problem and undertaking intelligence collection and target development; and
- contributing to appropriate legal, administrative and policy responses.[49]

4.81 The Committee notes that many of the strategies are activities that the Committee views as being part of the ACC's normal range of activities, for example, the last item 'contributing to appropriate legal, administrative and policy responses.'

4.82 Given that the submission indicates that in May 2003, the ACC board approved National ACC 'Intelligence Operations' for both Identity Crime and Card Skimming[50] the Committee would be expecting the Commission to be more positive in its strategic planning for this growth area.

4.83 Similarly, in the areas of money laundering and identity fraud, the ACC continues to pursue traditional strategies. Their suggested future directions include a large number of continuing activities such as consultations with AUSTRAC and the banks, in particular concerning the FATF's 40 recommendations, the use of Task Forces such as the Agio task Force, continuation of the work with AGEC and the former ABCI Identity Fraud register, and continued involvement in consultations concerning verification of identity documents. The more innovative suggestions include the establishment of a Task Force to investigate identity fraud.

4.84 While the Committee does not discount the effectiveness of traditional strategies the growth of crime in cyberspace suggests that to successfully combat it, LEAs may need to demonstrate a willingness to undertake new initiatives.

4.85 The Commission also mentions investigative techniques to include use of ACC Special Powers for production of documents and examination of witnesses. The Committee notes the special authorisation of the ACC Board for inquiries of this

---

48 Submission no.23, pp. 31-32

49 Submission no 23, p. 31

50 Submission no 23, p. 32

nature, but is apprehensive that these powers may be extended and become more commonplace than was initially envisaged.

Conclusion

4.86 The Committee notes that there is significant work being done on the international as well as the domestic level to minimize banking and credit card fraud, and to deal with money laundering. As with other aspects of cybercrime, there are two issues:

- education – to ensure the private and public users of this technology are aware of the risks and take steps to minimise them; and
- overall co-ordination and dissemination of relevant and timely information to the agencies involved.

4.87 The Committee considers that the proliferation of working parties, focus groups, interagency committees and similar groups has the potential to be more effective if there is an agency which can act as a co-ordinator of information and direct resources appropriately.

4.88 There is clearly a need to update the legislative base, which the Committee understands is occurring. The process should not stop at updating, as constant review is what is required to ensure that there is the ability to deal with the latest incarnation of attempts to damage the banking and finance environment.

4.89 Success in the detection and prosecution of cybercrime will depend on cooperation between Commonwealth and State Law Enforcement agencies, the financial institutions, as well as other agencies (such as AUSTRAC). The Committee considers that the formation of partnerships between these parties is crucial, if banking and monetary cybercrime is to be dealt with efficiently. In particular, government and private sector partnerships should be sought to disseminate important information regarding protection from financial fraud.

Chapter 5

Threats to national critical infrastructure

What is national critical infrastructure?

5.1 The term 'infrastructure' is a linguistic creation of the 20th century. Infrastructure is not confined to the public sector ownership of utilities but incorporates the services which organise and drive large corporations. It includes public utilities such as water, electricity and gas supplies, air-traffic control systems, banking and finance, telecommunications and transport systems.

5.2 A definition from the Australian Bankers' Association submission states:

> The Commonwealth has defined 'critical infrastructure' as that infrastructure which, if destroyed, degraded or rendered unavailable for an extended period, will significantly impact on the social or economic wellbeing or affect national security or defence. Clearly the banking sector is a vital component of the critical infrastructure. … but it must be appreciated that the banking sector is dependent upon at least two other components of the critical infrastructure, namely the electricity sector and the telecommunications sector.[1]

5.3 The Attorney General's Department submission observes that all of these structures are increasingly – if not exclusively – controlled by computers. Any system failure would seriously affect the Australian economy, and could threaten the safety and security of Australians.[2]

5.4 The Committee notes that some witnesses differentiated between the national information infrastructure and the national critical infrastructure.[3] However, their interdependency was highlighted in two examples given in the submission provided by the Australian Bankers' Association.[4]

5.5 The first example concerned damage to the main fibre optic cable between the US and China off the coast of Shanghai. It took four to five days to fix the problem, and the Chinese economy was rumoured to have lost many millions of dollars in lost transactions.

---

1 Submission no.19, p. 27

2 Submission no.21, p. 3

3 *Committee Hansard*, 17 July 2003, p. 3

4 Submission no 19, p.27

5.6 The second example concerned the Auckland power blackout in 1998. Due to failure of all the main cables supplying power to the inner city, hundreds of businesses were forced to shut down.

5.7 The Committee's view is that any threat to these interdependent areas has potentially grave consequences. There is clearly a relationship between threats to critical infrastructure and terrorism, which are briefly discussed below.

What are the threats and risks?

5.8 The ACC's submission gave an example of what is thought to be the world's first environmental vandalism case. The submission notes that this case is used world wide as an example of a critical infrastructure (hacking) attack:

> Between December 1999 and April 2000, the sewerage treatment facilities of Maroochydore Shire Council, Queensland, came under sustained electronic attack. That attack resulted in an environmental disaster which saw millions of litres of raw sewage spill into rivers, parks and the grounds of a Hyatt Regency hotel. The matter was forwarded to the Queensland Police for investigation.
>
> As a result an ex-employee, Vitek Boden, was intercepted by police in a vehicle which contained a laptop computer, with wireless access to the sewerage control system. He was later charged found guilty on 30 charges involving computer hacking, theft and causing significant environmental damage, in what was described as the world's first environmental vandalism case.[5]

5.9 A more recent example was related in evidence by the Victoria Police:

> Earlier this year the Victoria Police Tactical Response Squad sought the assistance of the Computer Crime Squad in the investigation of a Melbourne man who had forwarded threatening emails against Melbourne Water to the National Terrorist Hotline. This man made a series of threats that he would remotely detonate drums of cyanide submerged in water reservoirs. The offender was apprehended and has been charged with a number of serious offences.[6]

5.10 In the latter example, there was an effective response to the threat, and it is clear that the heightened awareness of the possibility of such threats played a large part in the effective apprehension of the perpetrator.

5.11 However, the Committee notes that the earlier example appears to have taken the victims by surprise. It is clear that there is a need to stay ahead of as many potential vulnerabilities as possible, which the Committee acknowledges in this most technically complex area is not simple. This is so particularly because criminals often

---

5 Submission no. 23, p.34

6 *Committee Hansard*, 17 July 2003, p.38

have access to large financial resources to assist with developing their technical expertise.

5.12 The ACC submission gave examples of potential areas of threat.[7] These include:

- Attacks or failures within information systems which may expose a vulnerability potentially affecting others in the sector.
- Hacking into a computer network by an individual.
- Distribution of malicious software (such as viruses) which enter computer systems in order to damage them.
- Denial of service attacks, where the internet ports or email of the target computer system is bombarded with data to prevent it from communicating.
- Redirection, or spoofing, of website traffic away from its intended destination.

5.13 The Committee learned that these activities can include nuisance worms, mass-mailing email systems, blended threats (which are threats which contain malicious code which attack vulnerabilities within a system) and the viruses such as Nimda, Code Red and the SQL Slammer worm, which Symantec told the Inquiry had the potential to bring down significant portions of the Internet backbone.[8]

5.14 In a report published in 2002,[9] the Office of Strategic Crime Assessment (OSCA– now part of the Australian Crime Commission (ACC)) noted that there were risks not only from electronic attack, but also from exploitation of software or procedural vulnerabilities. This included 'social engineering,'[10] a term which was used by several witnesses. In evidence PricewaterhouseCoopers explained:

> Social engineering is getting a person's confidence so that they may tell you information that you should not rightfully have.[11]

5.15 From the evidence given, it appeared to the Committee that this particular vulnerability would be difficult to overcome through purely technical means. The solution relies on protocols, and on human beings being aware of 'social engineering' attempts to obtain information, and resisting them. While organisations need to have clear guidelines regarding the preservation of crucial information, as well as defining the consequences of breaching the guidelines, there will always be the possibility of an unpredictable breach arising from 'the human factor'.

---

7 Submission no 23, p. 34

8 *Committee Hansard*, 18 July 2003, p.70

9 *Long-Term Criminal Risks to the National Information Infrastructure (NII),OSCA* 2002

8 Submission no. 12a; *Committee Hansard*, 17 July 2003, p.7

11 *Committee Hansard* 21 July 2003, p.64

Preventing infrastructure damage

5.16 Clearly, given the potential for damage to industry and the economy, the protection of critical national infrastructure is a matter of some concern. Symantec Australia gave a list of the matters considered important in determining a protection strategy:

> You have to identify what your key assets are, you have to identify where your threats, vulnerabilities and risks are, and then you have to take appropriate action and build systems around the bits and pieces of your system to make sure they all work together in harmony. … you have to prepare just in case everything goes wrong and look at business continuity management… it is not just one thing; it is a whole series of things.[12]

5.17 The Committee was concerned about just how realistic it is to expect global compliance with these standards, once established. Standards Australia's response was that a decision about where to exert security requirements comes down to having a cost-benefit basis for making that decision, because security is all about considering what you are trying to secure:

> There are trade-offs. The functionality is limited if you go for a higher rather than a lower level of security, and it is going to cost you more at the end of the day. … standards are a key issue [they] provide a language that allows you to communicate how you manage security.[13]

A view on best practice information security

5.18 In its submission, Symantec noted:

> With more than 85% of the world's critical infrastructure owned and operated by private entities, public/private cooperation is critical to securing our critical data from the rising incidence and impact of malicious activity.[14]

5.19 Symantec sets out its best practice strategies for 'government and enterprises'.[15] It summarises much of what was put to the Committee in submissions as well as in evidence. The strategies include:

- Security policies.
- Risk assessments.
- Standards, procedures, and metrics.
- Security roadmap.

---

12 *Committee Hansard*, 18 July 2003, pp. 49-50

13 *Committee Hansard*, 18 July 2003, pp. 50-51

14 Submission no 13, p.7

15 Submission no 13, p.8

- Selection and implementation of solutions.
- Training of security professionals and employees.
- Security management.
- Incident response and recovery.

Regional initiatives

5.20 Within the region, strategies for the protection of both the national critical infrastructure and the national information infrastructure are being studied within APEC. In evidence Mr Orlowski[16] noted that the critical infrastructure is the responsibility of APEC's counter-terrorism group.

5.21 The Committee heard that APEC's most important work in this area is ensuring that each economy or country has the capability for computer emergency response teams (CERT) to meet any emergency, and for developing a compendium of security standards. Both these tasks address strategies identified by Symantec.

5.22 While governments set their own standards, Mr Orlowski told the Inquiry:

> the extent of standards use within the private sector is very patchy between different organisations. A lot of our critical infrastructure is in fact operated by the private sector, so there is a need to ensure that they have guidance on the way they should be protecting this infrastructure on which we rely.[17]

National initiatives

5.23 The Attorney General's Department submission points out that NOIE (the National Office of the Information Economy) and the Attorney General's Department are the key agencies with policy responsibility for implementing the government's E-Security National Agenda. The operational agencies include the AFP, the Australian High Tech Crime Centre (AHTCC), the Australian Intelligence and Security Organisation (ASIO) and the Defence Signals Directorate (DSD). The Department also notes that additional agencies – including APRA, ASIC and the ACC – have been included in the establishment of AusCERT (the Australian Computer Emergency Response Team).

5.24 AusCERT was founded in 1992 and covers the private sector. The Attorney General's Department submission notes:

> AusCERT acts as a coordination centre, in an advisory capacity, as a centre of expertise and as a portal to its contacts throughout the world, for issues of computer security. AusCERT is part of the University of Queensland, and is

16 *Committee Hansard*, 17 July 2003, p. 3

17 *Committee Hansard*, 17 July 2003, p. 4

> a member of the Forum of Incident Reponses and Security Teams, a global organisation.[18]

5.25 AusCERT is partly funded by the Commonwealth government and raises other funds to cover its operating costs through member subscriptions and the provision of computer security training and education and consultancy services.[19] The Australian Crime Commission has recently provided funding support (along with other Commonwealth agencies) for a national incident reporting scheme and public alerts service, which will be provided free of charge to the Australian community.

5.26 The Committee was also told of a project jointly sponsored by AusAID (the Australian Aid Authority) and AusCERT. The project involves building computer emergency response team capacity in developing countries. Its purpose is to provide infrastructure to countries which might not have the level of expertise available to protect their own information infrastructure.[20]

5.27 The ABA told the Inquiry of the development of a banking and finance infrastructure advisory group which will report to the Critical Infrastructure Advisory Council (CIAC), an initiative established by the Attorney General and the Minister for Communications, Information Technology and the Arts. The Council's role is to oversee the sector advisory groups and provide advice to the Attorney-General on the national approach to protecting critical infrastructure.

5.28 The submission from the Attorney General's department explained that CIAC is a part of an initiative announced by the Prime Minister in November 2002. Alongside CIAC is the Trusted Information Sharing Network for Critical Infrastructure Protection (TISN).

> TISN is intended to allow the owners and operators of critical infrastructure to share information on important issues such as business continuity, consequence management, information system attacks and vulnerabilities, e-crime, protection of key sites from attack or sabotage, chemical, biological and radiological threats to water and food supplies, and the identification and protection of offshore and maritime assets.[21]

5.29 The Committee understands from the submission that TISN will use existing industry advisory groups from different sectors where possible. The Network is designed to promote a culture of trust 'based around shared threats and vulnerabilities'.[22] The Attorney General's Department anticipates that the advisory group will develop strong links to the equivalent US forums the Information Sharing and Analysis Centers (ISACs).

---

18 Submission no 21, p. 22

19 AusCert website: http://www.auscert.org.au

20 *Committee Hansard*, 17 July 2003, p.2

21 Submission no. 21, p.24

22 Submission no. 21, p.24

5.30 The Committee also noted from the submission provided by the Australian Bankers' Association that there is a proposal for TISN to include a number of Infrastructure Assurance Advisory Groups (IAAGS). These groups will be representative of particular sectors: for example, the ABA will be part of an IAAG for the finance sector.[23]

5.31 While the Committee welcomes a co-operative approach to infrastructure protection, it is aware that there is a need for a consistent approach to that protection.

Training

5.32 One of the keys to a consistent approach to protection and an identified element of the best practice strategies is training. During the inquiry the Committee was advised of some of the work being progressed in this area.

5.33 Mr Orlowski indicated in evidence that APEC is providing some training to the less developed economies in the region.[24] PricewaterhouseCoopers noted that technical training must be integrated with training in presenting technical findings to a court.[25]

5.34 This need was also acknowledged in the ACC's evidence which referred to the need for training and the necessity to have access to highly specialised knowledge. However the ACC also noted the need for:

> a coordinated and perhaps far more centralised or nationally driven level of expertise, while at the state level you have the skills that might be required for your own jurisdiction.[26]

5.35 The Committee notes that effectiveness in this area demands, (as with so many aspects of the responses to cybercrime) central co-ordination of both training and expertise. The Committee considers that establishment of a such a body preferably within an existing agency should be given a high priority.

5.36 The Committee also notes that this is a matter in which the public and private sectors must work together. Almost all witnesses noted the need for, and the initiatives being taken in, public/private sector co-operation and liaison.

5.37 The Committee is concerned that although there is a proliferation of potential solutions, and many groups which are addressing the issues, there lacks (as with the other areas which are the subject of this Inquiry) a central body which has the function of keeping track of potential threats and solutions; such an organisation could act as a clearing house for this information, ensuring that it was disseminated widely and

---

23 Submission no.19, p.28

24 *Committee Hansard*, 17 July 2003, p. 2

25 *Committee Hansard*, 21 July 2003, p.71

26 *Committee Hansard*, 18 July 2003, p.12

appropriately. Although the Committee sees the ACC and the AHTCC contributing to this task, it does not believe that a law enforcement agency is best suited to the task.

Role of the ACC

5.38 The ACC's contribution to prevention is in sharing its experience and its intelligence, as far as it is appropriate, with other agencies who develop these strategies.

5.39 The ACC submission notes[27] that historically, the NCA/ACC has only investigated attacks on critical infrastructure concerning organised crime. However the ACC now incorporates the Office of Strategic Crime Assessment (OSCA) which has the task, among others, of assessing all kinds of criminal threats, including those in cyberspace.

5.40 The commencement of a Cybercrime Program in 2001 under the ACC's predecessor, the NCA, highlighted the possibility of threats posed by organised criminal activity to both the Australian information and the physical infrastructures. The ACC sees its new functions – notably its role in advising the ACC Board on national criminal intelligence priorities – as well as maintenance of liaison and intelligence work as important parts of its role in combating organised crime.

5.41 The Committee notes that the ACC sees its multi-jurisdictional focus on the 'high end of criminality' as a 'unique tool to Australia's response to this high risk and emerging form of criminality'.[28] The ACC also perceives its coercive powers and national intelligence framework as invaluable in the investigation of critical infrastructure attacks especially against government institutions.

5.42 The Committee supports the ACC's view of its role within an area of criminality that is merging with terrorist threats to national security. However, the Committee notes the views of the Victorian Bar in evidence in discussing the proposal that monitoring warrants – similar to those available under the *Australian Security Intelligence Act 1979* (the ASIO Act) – be available to the ACC for cybercrime investigations. The Committee was advised that this power exists already under the ASIO Act in cases in which there is a threat to national infrastructure:

> Provided the suspected behaviour fits the definition of 'security' in section 4 of that [the ASIO] Act then the fact that the behaviour is being carried out by use of cybercrime techniques will not mean that government will not be able to deal with it provided it has the necessary impact on national security.[29]

---

27 Submission no 23. p. 34

28 Submission no 23, p. 34

29 *Committee Hansard*, 17 July 2003, p 23

5.43 The main focus of the work of the ACC is not on security but on the collection and processing of criminal information and intelligence, as set out in section 7A of the ACC Act (see Appendix 1). There is an ASIO representative on the ACC Board, which ensures an ongoing exchange of information and views at the highest level.

5.44 The ACC expressed some concern about its own vulnerabilities to attack and sees a solution in the formation of partnerships with other organisations. They include:

- AGEC (the Action Group into the law enforcement implications of Electronic Commerce) chaired by AUSTRAC, which has a focus on banking, money laundering and electronic payment systems.
- Information Infrastructure Protection Group (IIPG) chaired by AGD, with a focus on threats to the national critical infrastructure information.
- Electronic Security Coordination Group (ESCG), chaired by NOIE.
- AusCERT (Australian Computer Emergency Response Team) who have recently been contracted to provide Alerts and Warnings, and an Incident Reporting Scheme.[30]

5.45 The Committee notes the importance of the ACC's partnership approach, which as an intelligence sharing initiative will assist in keeping information about potential threats as up to date as possible. While part of the ACC is operationally directed towards major criminal activity, and apprehending the perpetrators, the former ABCI and OSCA, who have a research and intelligence focus have much to offer a partnership with other agencies.

5.46 The Committee also notes that the Commission acknowledges the need for the development of its own internal strategies which would minimise the effect of any attempt at exploitation of weaknesses in its information systems. The Committee encourages the Commission to give priority to this. However, while the Committee agrees that partnerships are necessary to combat cybercrime it would remind the ACC, and particularly the Board, of the need to continue to set its priorities within the context of its work programs.

Conclusion.

5.47 The evidence and the submissions presented to the Inquiry demonstrate a number of initiatives across both the private and the public sector aimed at minimising threats to critical infrastructure and at dealing with those which may occur. However, as with other areas within this Inquiry, there remains a need to ensure that all such initiatives are undertaken in an environment in which each interest group remains informed of the activities of the others.

30 Submission no. 23, p. 36

Chapter 6

Further Developments and Conclusion

Recent initiatives

6.1 The world wide growth of information systems has resulted in new crimes and novel ways to perpetrate old crimes. As with any new development, the response to these crimes has been at first almost ad hoc. The Committee is reassured to find during the inquiry that a systemic approach is emerging.

6.2 The internet is a global phenomenon and any regulation of its use needs to be international to have the greatest impact. Internationally, the United Nations have addressed the issues and provided the parameters in which governments can usefully contribute to the regulation of an industry that offers great communication benefits to its citizenry.

6.3 Since the Committee commenced its Inquiry there have been some developments in the regulation of the Internet, both within Australia and internationally.

6.4 These include:

- introduction into Federal Parliament of the Spam Bill 2003; and
- the closure of certain internet chat rooms by Microsoft.

The Spam Bill 2003

6.5 The Spam Bill 2003 (the Bill) resulted from a report released by the National Office for the Information Economy in April 2003. In response, the government has developed a number of initiatives, including an information campaign, and legislation.

6.6 The legislation focuses on:

- the regulation of 'commercial electronic messages'; and
- the prohibition on the sending of unsolicited commercial electronic messages (commonly referred to as spam).

6.7 The Bill provides amendments to relevant legislation which will allow the Australian Communications Authority (ACA) as the overseeing body, to monitor commercial electronic message activity. It will also investigate complaints.

6.8 The scheme will also have enforcement provisions as well as provisions for the development of relevant industry codes and standards relating to commercial electronic messaging The ACA can institute proceedings in the Federal Court for breaches of the Act. Significant monetary penalties can be imposed, and the Court can order compensation where a party has suffered damage due to the breach.

6.9 From the evidence given and the submissions provided to the Inquiry one of the clear messages is that legislation or policy initiatives must have an international focus as well as a domestic application. The Explanatory Memorandum states:

> The proposed framework contained in the Bill is aimed at reducing Australia as a source of spam, minimise spam for Australian end-users and extend Australia's involvement in worldwide anti-spam initiatives.[1]

6.10 The Committee notes that the effect of the Bill is not intended to be confined to the domestic sphere but to contribute to international anti- spam initiatives.

Internet Chat Rooms

6.11 In Chapter Three of this report, there was discussion of the concern about the use of chat rooms, and the fact that control of their content and activities is impractical. On 24 September 2003, Microsoft announced it would close its chat rooms in 24 countries on 14 October. The company will not be closing services in the United States, Japan,New Zealand, Brazil and Canada which are subscriber-based. The subscriber-based services are paid for by credit card and therefore any illegal activity is traceable.

6.12 The Committee notes that Microsoft said that it wished to 'create a safer and more secure online experience and we want to protect families, in particular children, from unsolicited information and inappropriate communication online'.[2]

6.13 The Committee is also aware from the same press report that some experts believe that this would not necessarily make any difference to Internet safety, and disadvantages the 300,000 Australian users who will no longer be able to use this facility.

6.14 While not in any way detracting from the possible effect of Microsoft's action, it is possible that those who engage in criminal activities in chat rooms will simply use other technology such as mobile phones, which are increasingly capable of becoming communication centres with all of the capabilities of telephone, internet, video and television combined. The activity is likely to be diverted but not eliminated.

Conclusion and recommendations

The ACC and the AHTCC

6.15 The Committee considers that the roles of the Australian High Tech Crime Centre (AHTCC) and the Australian Crime Commission (ACC) in cybercrime detection and enforcement should complement each other. The ACC's role in

---

1 *Spam Bill 2003;* Explanatory Memorandum, p. 1

2 McLennan, David *'Shut chat rooms no help for net safety,'* The Canberra Times, 25 September 2003

collection and dispersal of intelligence is a part of its enforcement role function: the ACC is not a security agency.

6.16 The AHTCC's can support this role in its monitoring of the technological aspects of criminal activity, and keeping agencies apprised of the latest technology as well as the ways in which it might be used to commit crime. As two Commonwealth authorities, one of which includes the ACC the involvement of the State and Territory jurisdictions, there is the potential to establish a co-operative network of communication to act as a powerful weapon against cybercrime.

6.17 During the Inquiry the Committee's attention was drawn to an article by Michael Sussmann published in the Duke Journal of Comparative and International Law.[3] Sussmann summarises the challenges and the responses necessary to achieve cross-jurisdictional control of cybercrime. He notes that the former US Attorney General Ms Janet Reno outlined four critical areas for attention: legislation, commitment of personnel and resources, improved global abilities and an improved regime for collecting and sharing information.

6.18 The four categories apply equally to the three aspects of cybercrime under consideration, and provide a framework for the ways in which the ACC and the AHTCC might approach their roles.

Legislation

6.19 In an area such as cybercrime where new technologies are constantly being developed and taken up to facilitate crime, the regular monitoring of the adequacy of current legislation is essential to the success of enforcing the law against cybercrime.

Commitment of personnel and resources

6.20 As information technology becomes a part of the routine of everyday life, it will become part of crime. The current distinction between 'old' crime and e-crime will become blurred as it becomes a part of every crime. Without a commitment to training law enforcement personnel now, the capacity of LEA to respond to these developments will be diminished. Resources for education as well as those to ensure that the law enforcement bodies are apprised of all the available technological devices and information are necessary to meet this requirement.

Recommendation 7

The Committee recommends that the Government include in its cybercrime strategy, directed training for law enforcement agencies, and the development of a whole of government approach in which individuals can gain expertise which can be shared between those agencies.

---

3 Sussmann, Michael A. The Critical Challenges from International High Tech and Computer Related Crime at the Millennium [Vol 9:4511999]

6.21 Further, the Committee believes that education should include public education, as well as that of the law enforcement agencies.

Improved global abilities

6.22 Australia's acceptance of its role in the international arena was demonstrated during the inquiry. The recently introduced SPAM Bill (see paragraphs 6.5 to 6.9) acknowledges its responsibilities. Further, Australia's participation in the work of APEC is an example of the initiatives being undertaken in the global arena. In addition, the networks established by organisations such as the AFP, the AHTCC and the ACC are vital to Australia's participation in a consistent international approach.

Improved regime for collecting and sharing information.

6.23 The Committee has made recommendations in recognition of the need for a consistent national approach to ensuring that all relevant information is available to the agencies which need it. It is clear that there are opportunities for all law enforcement agencies to collect information on technology and crime and in doing so identify trends. Unless that information is shared, there is potential for duplication of activity leading to waste of resources and time. This is also contrary to the acknowledged need for a whole of government approach to combating cybercrime.

6.24 The Committee considers it is clear that isolated state or national action cannot succeed in controlling any other aspect of cybercrime unless there is a global commitment to a consistent regime of legislation and regulation. These areas for development can be applied at the local (multi- jurisdictional) Australian level, as well as the international level. With its international relationships with similar bodies, and its multi-state representation, the ACC is ideally placed to contribute to developing that regime, but not necessarily leading it.

Recommendation 8

The Committee recommends that the Australian Crime Commission continue its current level of involvement in cybercrime investigation, and intelligence gathering, as well as further developing its international liaison role.

Recommendation 9

The Committee recommends that the Australian Crime Commission ensure its information sharing strategies, including liaison with the Australian High Tech Crime Centre, maximise the opportunities for giving and receiving accurate and timely information about cybercrime methods and technology.

6.25 It became clear during the course of the hearings that there is no co-ordinating body which combines the role of watchdog, investigator, and prosecutor in this area. In his evidence to the Committee, Mr Melick said:

> The trouble is that there are too many players and no overarching coordinator.[4]

6.26 There is no organisation which is across all of the associated issues. While the Committee acknowledges that in other contexts combining these roles may not be desirable, the nature of cybercrime is such that rapid response is essential.

6.27 The Australian Federal Police submission noted that the new AHTCC has, as part of its role, to provide a national co-ordinated approach to combatting serious complex and/or multi-jurisdictional high tech crimes. In addition it also assists in improving the capacity of all jurisdictions to deal with high tech crime. The Committee is of the view that the AHTCC is in a position which would enable it to take a national perspective on cybercrime. However in order to develop this capacity, there must be a framework which supports it.

6.28 The Committee observed that Sussmann sets out this framework as including:[5]

- High technical standards which preserve public safety.
- The ability to preserve critical traffic data routinely, with powers to require a longer period of storage.
- The ability to share information across jurisdictions quickly – this requires legal processes supplemented by administrative procedures to facilitate the sharing of data.
- Government-Industry co-operation. This involves government minimising the compliance burden on industry, and simultaneously industry considering the public safety and interest as being a top priority.

6.29 From the Committee's observations of the evidence and the submissions provided, there are many ways in which LEA's, government agencies and the private sector are already working within Sussman's framework. However, it believes that further work can be done at all levels and in all spheres to develop strategies that will initiate innovative measures against cybercrime, and respond rapidly to instances of cybercrime. The complementary roles for the ACC and AHTCC can be identified in the following recommendations which are designed to promote partnerships in this process of Commonwealth and State governments as well as private industry.

Recommendation 10

The Committee recommends that the Australian Crime Commission seek out opportunities to participate in appropriate public/private sector cybercrime projects, to promote the sharing of information, and the efficient prevention and investigation of cybercrime offences.

---

4 *Committee Hansard*, 21 July 2003, p. 30

5 Sussmann, pp. 468 -469

Recommendation 11

The Committee recommends that the Australian High Tech Crime Centre act as a clearing house for information on cybercrime, in order to explore initiatives to combat it.

6.30 The Committee believes that the ACC can make an important contribution to the law enforcement agencies' understanding and prosecution of cybercrime in a number of ways:

- Through its statutorily authorised intelligence gathering function, the ACC can share its intelligence in the area with other agencies. In particular, through its Board, State Police can remain informed of these activities at the highest level.
- The ACC can work with the AHTCC on the prevention and investigation of cybercrime through the ACC's knowledge of the operational environment, and the AHTCC's knowledge of advancing technology.

6.31 The Committee observed with some optimism that developments in providing that protection are occurring in all areas: legislative, both private and public sectors, law enforcement agencies, and with the Internet Service Providers themselves. It is clear to the Committee that there are serious and sustained efforts being made to counter cybercrime, and the recommendations contained in this report are designed to enhance that effort.

APPENDIX 1

Sections of *Australian Crime Commission Act 2002* and *Australian Federal Police Act 1979*

Australian Crime Commission Act 2002

Section 7A

> **Functions of the ACC**
>
> The ACC has the following functions:
>
> (a) to collect, correlate, analyse and disseminate criminal information and intelligence and to maintain a national database of that information and intelligence;
>
> (b) to undertake, when authorised by the Board, intelligence operations;
>
> (c) to investigate, when authorised by the Board, matters relating to federally relevant criminal activity;
>
> (d) to provide reports to the Board on the outcomes of those operations or investigations;
>
> (e) to provide strategic criminal intelligence assessments, and any other criminal information and intelligence, to the Board;
>
> (f) to provide advice to the Board on national criminal intelligence priorities;
>
> (g) such other functions as are conferred on the ACC by other provisions of this Act or by any other Act.

'Federally relevant criminal activity' is defined in section 4 of the Act and includes cybercrime as a serious and organised crime offence.

> (a) a relevant criminal activity, where the serious and organised crime is an offence against a law of the Commonwealth or of a Territory; or
>
> (b) a relevant criminal activity, where the serious and organised crime:
>
> > (i) is an offence against a law of a State; and
> >
> > (ii) has a federal aspect.

Section 4 also defines serious and organised crime as an offence:

(a) that involves 2 or more offenders and substantial planning and organisation; and

(b) that involves, or is of a kind that ordinarily involves, the use of sophisticated methods and techniques; and

(c) that is committed, or is of a kind that is ordinarily committed, in conjunction with other offences of a like kind; and

(d) that is a serious offence within the meaning of the Proceeds of Crime Act 2002, an offence of a kind prescribed by the regulations or an offence that involves any of the following:

…

(xix) cybercrime;

Australian Federal Police Act 1979

Section 8
Functions

1) The functions of the Australian Federal Police are:

…

(b) the provision of police services in relation to:

(i) laws of the Commonwealth;

(ii) property of the Commonwealth (including Commonwealth places) and property of authorities of the Commonwealth; and

(iii) the safeguarding of Commonwealth interests;

…

(c) to do anything incidental or conducive to the performance of the foregoing functions.

APPENDIX 2

List of Submissions

1. Xtec Inc (Australia)
2. Mr Darren Brookes (private capacity)
3. Tri-M Systems Inc.
4. Electronic Frontiers Australia Inc.

4a. Electronic Frontiers Australia Inc (Supplementary)

5. CONFIDENTIAL

5a Australian Securities and Investments Commission

6. The Law Society of Western Australia
7. Australian Institute of Family Studies
8. Curtin University of Technology
9. Orlowski Consulting
10. New South Wales Council for Civil Liberties Inc.
11. Standards Australia International Ltd
12. CONFIDENTIAL

12a PricewaterhouseCoopers

13. Symantec Australia
14. Mr Tony Healy (private capacity)
15. Australian Broadcasting Authority
16. Mr Graeme Bond (private capacity)
17. NSW Police
18. Australian Institute of Criminology
19. Australian Banker's Association

20. Mr Martin Hanson (private capacity)

21. Attorney-General's Department

22. Mr Brendan Scott (private capacity)

22a Mr Brendan Scott (private capacity – supplementary)

23. Australian Crime Commission

24. Queensland Police Service

25. Victoria Police

26. Australian Federal Police

27. Australian Transaction Reports and Analysis Centre (AUSTRAC)

28. The Victorian Bar

29. Mr Greg Melick (private capacity)

30. Internet Industry Association

31. Mr Julian Winch (private capacity)

APPENDIX 3

Witnesses who appeared before the Committee at public hearings

Thursday, 17 July 2003
Legislative Council Committee Room, Parliament House, Melbourne

Mr Steve Orlowski (Private capacity)

The Victorian Bar and the Criminal Bar Association
Mr Edwin Lorkin, Barrister

Australian Institute of Family Studies
Dr Janet Stanley, Acting Research Fellow

Victoria Police
Detective Acting Superintendent Richard Grant, Acting Manager, Organised Crime Investigation Division
Detective Superintendent Philip Masters, Major Fraud Investigation Division
Detective Acting Inspector Christopher O'Connor, Sexual Crimes Squad
Detective Senior Sergeant Peter Francis, Officer in Charge, Computer Crime Squad

Mr Graeme Bond (Private capacity)

Friday, 18 July 2003
Commonwealth Parliament Offices, Sydney

Australian Crime Commission
Mr Alastair Milroy, Chief Executive Officer
Mr Scott McLeod, Coordinator, National Cybercrime Unit

Australian Broadcasting Authority
Professor David Flint, Chairman
Mr Richard Fraser, Assistant Manager, Content Assessment Section, Hotline Manager

Mr Brendan Scott (Private capacity)

Australian Bankers Association
Mr Tony Burke, Director
Mr John Geurts, Executive General Manager, Group Security, Commonwealth Bank of Australia

Standards Australia
Mr Mark Bezzina, Business Standards
Mr Brahman, Project Manager, Communications, IT and e-Commerce Standards

Australian Transaction Reports and Analysis Centre
Mr Neil Jensen, Director
Ms Liz Atkins, Deputy Director, Money Laundering Deterrence

Symantec Australia
Mr John Donovan, Managing Director
Mr David Banes, Regional Manager, Security Response

New South Wales Police
Ms Gillian O'Malley, Manager (adviser to Executive)
Detective Inspector William Vander Graaf, Coordinator, Computer Crime Unit and Fraud Crime Team

Monday, 21 July 2003
Parliament House, Canberra

Professor Peter Grabosky (Private capacity)

Australian High Tech Crime Centre
Federal Agent Alastair MacGibbon, Director
Mr Nicholas Klein, Team Leader, Intelligence Development

Australian Securities and Investments Commission
Mr Keith Inman, Director, Electronic Enforcement

Electronic Frontiers Australia Inc.
Ms Irene Graham, Executive Director

PricewaterhouseCoopers
Mr Graham Henley, Director
Mr Scott Pobihun, Manager

Attorney-General's Department
Mr Bruce Bannerman, Principal Legal Officer
Mr Trevor Clement, Assistant Secretary, Critical Infrastructure Protection
Mr Geoff McDonald, Assistant Secretary, Criminal Law Policy
Mr Michael Rothery, Director, Critical Infrastructure Policy, Critical Infrastructure Protection Branch
Mr Anton Schneider, Acting Assistant Secretary, Strategic Law Enforcement Branch
Ms Kelly Williams, Principal Legal Officer, Criminal Law Branch

APPENDIX 4

The United Nations Resolution of the General Assembly no. 55/63 'Combating the Criminal Misuse of Information Technologies'

(*a*) States should ensure that their laws and practice eliminate safe havens for those who criminally misuse information technologies;

(*b*) Law enforcement cooperation in the investigation and prosecution of international cases of criminal misuse of information technologies should be coordinated among all concerned States;

(*c*) Information should be exchanged between States regarding the problems that they face in combating the criminal misuse of information technologies;

(*d*) Law enforcement personnel should be trained and equipped to address the criminal misuse of information technologies;

(*e*) Legal systems should protect the confidentiality, integrity and availability of data and computer systems from unauthorized impairment and ensure that criminal abuse is penalized;

(*f*) Legal systems should permit the preservation of and quick access to electronic data pertaining to particular criminal investigations;

(*g*) Mutual assistance regimes should ensure the timely investigation of the criminal misuse of information technologies and the timely gathering and exchange of evidence in such cases;

(*h*) The general public should be made aware of the need to prevent and combat the criminal misuse of information technologies;

(*i*) To the extent practicable, information technologies should be designed to help to prevent and detect criminal misuse, trace criminals and collect evidence;

(*j*) The fight against the criminal misuse of information technologies requires the development of solutions taking into account both the protection of individual freedoms and privacy and the preservation of the capacity of Governments to fight such criminal misuse;

[the General Assembly]

2. *Invites* States to take into account the above-mentioned measures in their efforts to combat the criminal misuse of information technologies;

3. *Decides* to maintain the question of the criminal misuse of information technologies on the agenda of its fifty-sixth session, as part of the item entitled 'Crime prevention and criminal justice'.

APPENDIX 5

Cybercrime: Commonwealth legislation[1]

The Australian Crime Commission Act 2002 establishes the ACC as an intelligence collection and dissemination body, for cybercrime offences (among others).

Criminal Code Act 1995 incorporates the Cybercrime Act – Computer Offences and law enforcement powers, fraud offences and other crimes which may be committed using information technology.

Classification (Publications, Films, and Computer Games) Act 1995 – complements State classification legislation.

Customs Act 1901 – covers import and export of child pornography.

Electronic Transactions Act 1999 regulates the use of electronic transactions.

Financial Transactions Reports Act 1988 establishes AUSTRAC, and the framework for the collection and analysis of financial intelligence .

Mutual Assistance in Business Regulation Act 1992 allows ASIC, the ACCC and APRA to provide assistance to foreign regulators, but not to gather evidence for criminal prosecutions.

Mutual Assistance in Criminal Matters Act (1987) allows Australia to provide prosecution material to countries with which it has no formal treaty-based relationship.

Payment Systems Regulation Act 1998 regulates payments systems such as credit and debit cards and stored value cards.

Proceeds of Crime Act 2002 allows courts to deal with assets which, on the balance of probabilities, are proceeds of crime or were acquired by a person who has engaged in criminal activities in the previous six years.

Privacy Act 1988 protects the collection storage and use of personal information.

Telecommunications Act 1997 requires telecommunications carriers to endeavour to prevent their facilities from being used to commit offences against the laws of the Commonwealth, States and Territories.

---

1 Submission no. 19, Australian Bankers' Association pp.30ff.

The *Telecommunications (Interception) Act 1979* was amended in 2002 to allow telecommunications interception warrants to be sought for child pornography related offences.