6

Criminal and Law Enforcement Framework

Introduction

6.1 The chapter discusses the existing criminal law framework intended to combat cyber crime and canvasses Australia's possible accession to the Council of Europe Convention on Cybercrime. The chapter concludes that Australian criminal law (substantive and procedural) is well developed but that legal policy in this field must ensure an appropriate focus on the transnational nature of cyber crime and particular challenges of digital evidence. There is also a strong case for a more strategic focus on the disruption of botnets and prosecution of botherders that will require intense international cooperation.

Criminal Law

6.2 Over the last decade, successive Australian Governments have enacted specific offences for the misuse of computers and telecommunications systems and online sexual abuse of children in the *Criminal Code Act 1995* (the Criminal Code).[1]

6.3 The technological aspects of cyber crime also pose particular challenges to the investigation of crimes against computers or that use communication

---

1 AFP, *Submission 25*, p.13.

technologies.[2] In response to these challenges the law now provides police authorities with specific powers to obtain evidence to aid the investigation and prosecution of online offenders.[3]

6.4 The next section outlines some of the key provisions and canvasses witnesses' views on the adequacy of existing offences. The procedural aspects are then discussed in the following sections.

Computer Offences

6.5 The *Cybercrime Act 2001* (Cth) introduced computer offences into the Commonwealth *Criminal Code Act 1995* (Criminal Code) with maximum penalties ranging from two to ten years imprisonment.[4] The offences address the problems of hacking, denial of service attacks and malware intrusions. The offences follow those contained in the Model Criminal Code recommended by the Model Criminal Code Officers Committee of the Standing Committee of Attorneys-General (MCLOC).[5] A summary of the provisions is set out in appendix D.

6.6 The Constitution does not grant the Commonwealth express power over criminal activity *per se*, however, the Parliament can validly make laws to create criminal offences and provide for their investigation, prosecution and punishment, provided that the offences fall within, or are incidental to the exercise of a constitutional head of power.[6] In the context of cyber crime the Commonwealth offences apply only to the:

- protection of Commonwealth computers and computer systems; and
- the commission of crimes by means of a telecommunications service.[7]

6.7 However, State and Territory computer offences apply generally in the respective jurisdictions and therefore provide national coverage.[8]

---

2 Russell Smith, *Impediments to the Successful Investigation of Transnational High Tech Crime*, Trends and Issues in Crime and Criminal Justice No. 285, Australian Institute of Criminology, October 2004, p.1.

3 Attorney-General's Department, *Submission 44,* p.16; *Telecommunications (Interception and Access) Act 1979* (Cth)*; Crimes Act 1914* (Cth).

4 Part 10.7 Divisions 477 and 478 of the Criminal Code; AGD, *Submission* 44, p.18.

5 Model Criminal Code Officers Committee of the Standing Committee of Attorneys-General, Chapter 4 Damage and Computer Offences, Report of the Committee, February 2001.

6 Commonwealth criminal law is ancillary to the performance of the Commonwealth of its powers to protect itself, the Constitution, its institutions and to enforce its own laws; Sir Garfield Barwick, Crimes Bill 1960, Second Reading Speech, House of Representatives, *Debates*, 8 September 1960 pp.1020-1021 reported in *Research Paper No.12,* Department of Parliamentary Library, Canberra, 2002, p.4.

7 AGD, *Supplementary Submission 44.2*, p.10.

Identity Fraud Offences

6.8 The computer offences may be combined with Commonwealth or State or Territory provisions that cover identity related crimes, such as fraud, forgery, or dishonest dealing in personal financial information.[9]

6.9 The fabrication or misuse of identity has traditionally been treated as an aspect of these primary offences. In March 2008, the MCLOC recommended the introduction of specific identity fraud offences and a certificate for victims to assist in re-establishing their credit worthiness. The model offences do not require that a crime, such as theft, fraud, forgery or deception be perpetrated but merely that there is an intention to commit or facilitate the commission of an indictable offence.[10]

6.10 At the Commonwealth level, the House of Representatives passed the Law and Justice Legislation Amendment (Identity Crimes and Other Measures) Bill 2008 (the Bill) on 23 February 2009 and, at the time of writing, the Bill remains under consideration by the Senate. The Bill inserts three identity fraud offences into a new Part 9.5 of the Criminal Code. The offences are described in Appendix E.

6.11 The amendments also allow a person who has been the victim of identity crime to apply to a magistrate for a certificate to show they have had their identity information misused. The purpose of the certificate is to assist victims 'negotiating with financial institutions to remove fraudulent transactions, and other organisations such as Australia Post, to clear up residual problems with identity theft'.[11]

6.12 At the State level, both South Australia (SA) and Queensland have specific identity theft/fraud offences.[12] In March 2009, the Victorian Parliament passed the *Crimes Amendment (Identity Crime) Act 2009* (Vic). By December 2009, NSW had passed the *Crimes Amendment (Fraud, Identity and Forgery Offences) Act 2009* (NSW). The WA Criminal Code Amendment (Identity

8 AGD, *Supplementary Submission 44.2*, p.10; Microsoft Australia, *Submission 35*, p.7.

9 For example, section 480.4 of the Commonwealth Criminal Code makes it an offence to dishonestly obtain or deal in personal financial information without consent of that person to access funds, credit or other financial benefits.

10 MCLOC, *Final Report: Identity Crime*, Commonwealth of Australia, 2008.

11 AGD, *Supplementary Submission 44.1*, p.3.

12 AGD, *Submission 44*, p.4; *Criminal Law Consolidation (Identity Theft) Amendment Act 2003* (SA); *Criminal Code and Civil Liability Amendment Act 2007* (Qld); Note that under section 144B of the *Criminal Law Consolidation Act 1935* (SA) it is an offence to assume a false identity or falsely pretend to be entitled to act in a particular capacity. Unlike the model provisions this offence does not require proof of an intention to commit a serious criminal offence.

Crime) Bill 2009 is currently before the WA Parliament.[13] There was no evidence indicating whether Tasmania, the Northern Territory or the Australian Capital Territory have or are soon to adopt the model offences.

Commentary

6.13 The Australian Federal Police expressed the view that criminal offences to tackle cyber crime are sufficient, the difficulty lies more in enforcement and the trans-national nature of most cyber crime.[14] The AGD also said that while some aspects of the law and law enforcement could be strengthened existing Australian laws are 'appropriate'.[15] Nevertheless, some questions were raised about the breadth and uniformity of the computer offences.

Technology Neutral Language

6.14 The Committee was told that computer offences need to be drafted in technology neutral language to minimise repeated amendment of the Criminal Code.[16] According to AGD, the Part 10.7 offences are drafted so as to apply as technology evolves:

> For example, the term "computer" was not defined to ensure the computer offences will encompass new developments in technology, for example, mobile phones that allow access to the Internet.[17]

6.15 The Internet Industry Association (IIA) were satisfied that legitimate investigations carried out to determine the level of security of a client's system would not be caught by the offence provisions.[18] However, Symantec were concerned that legitimate software suppliers must not be inadvertently committing offences when 'using tools/devices for

13 The WA Bill 'utilises and builds upon (but does not specifically implement) the model provisions'; WA Legislative Council, *Standing Committee on Uniform Legislation and Statutes Review Report No 44*, March 2010, p. 14, viewed 17 March 2010, <http://www.parliament.wa.gov.au/parliament/commit.nsf>.

14 AFP, *Submission 25*, p.9.

15 AGD, *Submission 44*, p.7; The E-Security Review did recommend: agency collaboration to address 'legal issues associated with the blocking of user access to Internet sites by law enforcement and other agencies'; better coordination of crime reporting; and training and information for the legal profession.

16 AGD, *Supplementary Submission 44.2*, p.10.

17 AGD, *Submission 44*, p.4.

18 IIA, *Submission 54,* p.2.

legitimate business purposes, e.g. conducting research, penetration testing, and/or supplying patches for vulnerabilities'.[19]

6.16 It was suggested that ss.478.3 and 478.4 clarify that it is only a criminal offence when the 'device has been developed primarily, deliberately and for the sole purpose of committing an offence'.[20] Other factors that should be considered include:

- whether the device is available on a wide scale commercial basis and sold through legitimate channels;
- whether the device is widely used for legitimate purposes with a substantial installation base; and
- the context in which the device was used to commit the offence compared with its original intended purpose.[21]

6.17 Symantec also questioned the scope of the term 'data' and argued that it should be clarified so it is clear that it includes malicious devices and tools and toolkits.[22]

6.18 A further question arose as to whether the placing and later exploitation of a latent functionality in computer hardware or software without the owner's knowledge or consent was caught by existing criminal provisions. The AGD assured the Committee that the computer offences adequately cover such conduct.[23]

Uniformity of Commonwealth, State and Territory Provisions

6.19 Some witnesses raised concern about the apparent inconsistency of computer offences across Australian jurisdictions. For example, Microsoft Australia submitted that New South Wales, Victoria, South Australia, the Northern Territory and the Australian Capital Territory have implemented the Model Criminal Code and established computer offences materially similar to the federal provisions.[24]

6.20 However, Queensland, Tasmanian and Western Australian regimes were described as 'less aligned with the Model Criminal Code; they appear to focus on computer hacking and misuse offences'.[25] The Tasmanian

19 Symantec, *Supplementary Submission 32.1*, p.2.
20 Symantec, *Supplementary Submission 32.1*, p.2.
21 Symantec, *Supplementary Submission 32.1*, p.2.
22 Symantec, *Supplementary Submission 32.1*, p.2.
23 AGD, *Supplementary Submission 44.1*, p.1.
24 Microsoft Australia, *Submission 35*, p.7.
25 Microsoft Australia, *Submission 35*, p.7

Government also noted that as most e-security threats involve the use of communications technology, most of the reforms have been at the national level.[26] The Australian Banker's Association (ABA) said that:

> Various provisions of the Model Criminal Code have, we believe, been sporadically and not necessarily consistently implemented across the Australian jurisdictions.[27]

6.21 In 2004 the Parliamentary Joint Standing Committee on the Australian Crime Commission recommended that the Commonwealth, State and Territory Attorneys-General give priority to implementing consistent cyber crime offence and evidence legislation.[28] The ABA was critical that this has not yet been fully realised.[29]

Committee View

6.22 The evidence to the Committee indicated that there has been considerable reform in the criminal law to adapt Australia's legal framework to the growth of malicious attacks against computers and computer systems. More recently the Attorneys-General have initiated improvements to ensure that identity theft/fraud is properly criminalised.

6.23 However, there is a need to maintain responsiveness to cyber crime and a dedicated cross jurisdictional working group is probably warranted. The idea for a working group is discussed at the end of this chapter.

6.24 The Committee is concerned with the current issue of uniformity of computer offences and those relating to identity fraud, which appears to be a continuing matter of concern. Lack of uniformity in Australian law makes both domestic and international cooperation more complex and inefficient. This is an issue that requires attention by the Attorneys-General of the Commonwealth and the State and Territory Governments.

6.25 On the scope of the existing provisions, the Committee believes that Symantec has expressed a legitimate concern that IT corporations and their staff could be exposed to possible criminal liability for possession, control, production or supply of 'data' (ss.478.3 and 478.4). However, each of these offences requires the prosecution to prove to the criminal standard (beyond reasonable doubt) that the possession, control,

---

26 Tasmanian Government, *Submission 51*, p.4.

27 ABA, *Submission 7*, p.7.

28 Parliamentary Joint Committee on the Australian Crime Commission, *Cybercrime,* March 2004, p.vii and p.15.

29 ABA, *Submission 7*, p.7.

production or supply of data was with intent to commit a computer offence. The Committee considers that, when all the elements are read together, the risk of mistaken prosecution or wrongful conviction is extremely remote.

6.26 On a related point, the Committee notes that intercepting communications is criminalised by the *Telecommunications (Interception and Access) Act 1979* (Cth). Recently proposed amendments are intended to ensure public and private network owners and operators can carry out 'computer network protection' activities such as using virus protection software without violating the prohibition on interception.[30]

Recommendation 8

That the Federal, State and Territory Attorneys-General review the existing computer and identity fraud provisions and, if necessary, introduce or amend provisions to ensure consistency across all Australian jurisdictions.

Law Enforcement Powers to Obtain Digital Evidence

6.27 The AFP told the Committee that the major challenge to domestic and foreign law enforcement agencies (LEAs) is the dynamic and trans-national nature of cyber crime. Some of the current key issues are:

- the ability to identify offenders who may be located in a different country to the victim and who can use technology to disguise their identity;
- the ability to quickly preserve, search and seize digital information, especially that protected by encryption or located in another country; and

30 *Telecommunications (Interception and Access) Amendment Bill 2009*; see also, AGD, *Discussion Paper and Exposure Draft Legislation: Computer Network Protection*, July 2009; The Senate Legal and Constitutional Affairs Legislation Committee, *Telecommunications (Interception and Access) Amendment Bill 2009 [Provisions]*, November 2009.

- the need for higher levels of international cooperation than that generally required for more traditional offline crimes.[31]

6.28 The convergence of new technologies, in particular, the growth of peer to peer and mobile phone technology was also identified as an additional challenge to shutting down botnets and collecting digital evidence for prosecution.[32] In particular, the AFP said that the ability of criminals to commit or facilitate offences through the use of disposable ICTs - such as prepaid mobile and wireless communications and free g-mail electronic addresses - will also restrict the ability of LEA's to obtain evidentiary material.[33]

Crimes Act 1914 (Cth) – Investigative Powers

6.29 Part IAA of the *Crimes Act 1914* (Cth) contains provisions which allow a law enforcement officer to search and seize electronic data. This includes provision for police to obtain an order to compel a suspect to access or provide assistance to access data that is evidence of the suspected offence. For example, revealing encryption keys or decryption data to enable police to obtain crucial evidence.[34]

6.30 It is currently an offence to fail to provide reasonable assistance to an LEA officer to access data stored on a computer at a search warrant premises (e.g. where the data is password protected or encrypted). The penalty is a maximum of six months imprisonment. The AGD advised that the Crimes Legislation (Serious and Organised Crime) Bill No.2 will amend the offence and increase the penalty from six months to two years.[35]

6.31 The *Crimes Act 1914* (Cth) also facilitates 'undercover' investigations. Part IAB allows a law enforcement officer to commit criminal offences as part of a controlled operation to investigate offences (including computer offences).[36] Part IAC allows law enforcement officers to use a false identity to investigate computer and telecommunications offences.[37]

---

31 AFP, *Supplementary Submission 25.1*, p.8; Russell Smith, *Impediments to the Successful Investigation of Transnational High Tech Crime*, Trends and Issues in Crime and Criminal Justice No. 285, Australian Institute of Criminology, October 2004, pp.1-6.

32 CLPC, *Submission 62*, p.3.

33 AFP, *Supplementary Submission 25.1*, pp.8-9.

34 Section 3LA of *the Crime Act 1914 (Cth).*

35 AGD, *Supplementary Submission 44.2*, p.8.

36 The offence must carry a maximum penalty of three or more years.

37 AGD, *Submission 44*, p.19.

Telecommunications (Interception and Access) Act 1979 (Cth)

6.32 The *Telecommunications (Interception and Access) Act 1979* (Cth) (TIA Act) has also undergone significant reform and allows for the interception of communications and access to historic and real time data.[38] However, the AFP said the capacity of some telecommunications carriers to meet their obligations under the TIA Act is insufficient and inhibits police investigations. In particular, some carriers have limited technical capacity to provide information required of them under the TIA. This information includes subscriber details, call log details and IP addresses.[39]

6.33 The TIA Act is administered by the Telecommunications and Surveillance Law Branch of the AGD. The TIA Act created the Communications Access Coordinator (CAC), who is the first point of contact for the telecommunications industry, LEAs and national security agencies:

> To assist industry to comply with their obligations, they are required to provide an interception capability plan on an annual basis which is assessed by law enforcement and national security agencies before being approved by the CAC. These plans outline how industry will meet their obligations under the TIA Act. The plans for 2009 have been approved and carriers range from very large organisations such as Telstra or Optus to smaller operators like Clear Networks. While some carriers have less capability, the CAC works with carriers to ensure they improve their capabilities as they grow their business.[40]

6.34 The Branch also administers an outreach program which 'provides extensive liaison and education for industry':

---

38 In 2005 the TIA was reviewed by Mr Anthony Blunn AO. The report, tabled in Parliament on 14 September 2005, recommended that legislation dealing with access to telecommunications data for security and law enforcement purposes be established, viewed 23 March 2010, <http://www.ag.gov.au/www/agd/agd.nsf/Page/Publications_Blunnreportofthereviewoftheregulationofaccesstocommunications-August2005>. The TIA was amended in 2006 to establish a warrant regime for access to stored communications. In 2007 the TIA was further amended to implement a two-tier regime for access to historic and prospective (real-time) telecommunications data. The provisions of the *Telecommunications Act 1997* (Cth), that regulated access to telecommunications data for national security and law enforcement purposes, were also transferred to the TIA. See, Sue Harris-Rimmer, Telecommunications (Interception) Bill 2006, Bills Digest No. 102, 2005–06, 28 February 2006, Parliamentary Library; and, Bronwyn Jaggers, Telecommunications (Inception and Access) Amendment Bill 2008, Bills Digest No. 71, 7 March 2008 for further detail.

39 AFP, *Supplementary Submission 25.1*, p.9.

40 The Communications Access Coordinator is a statutory position performed by the First Assistant Secretary of the National Security Law and Policy Division in AGD; AGD, *Supplementary Submission, 44.2*, p.3.

> The program involves the provision of legal advice to industry on their obligations under the Act. Additionally, TSLB provides face to face assistance for carriers, carriage service providers and ISPs. These programs enable AGD to assist industry meet their obligations under the legislation and provide a foundation of co-operation in the provision of assistance to law enforcement.[41]

Surveillance Devices Act 2004 (Cth)

6.35 The NSW Police argued that remote access under warrant would allow for surveillance at the point before encryption occurs:

> A broader issue relating to cyber crime is police powers, such as 'remote access powers'. By allowing a warrant to be obtained for remote access, law enforcement is more likely to be able to decipher encrypted data by conducting surveillance at a point between the user and the encryption interface. This would involve remotely accessing (or 'hacking into') a computer via the internet to obtain transmissions of product passing over that computer at a point at which it is unencrypted. This would require legislative amendments both at a State and Commonwealth level.[42]

6.36 According to AGD this form of surveillance raises a range of technical, legal and privacy issues which have to be assessed against existing laws. For example, the use of a remote surveillance device may amount to interception under the TIA Act or violate the Criminal Code.

6.37 Additionally, it is the TIA Act which provides a national regime to regulate highly intrusive investigative powers, whereas the *Surveillance Devices Act 2004* (Cth) does not provide a national regime. In turn, this raises jurisdictional issues when such devices are deployed across inter-state boundaries.[43]

6.38 The Committee was told that a working group, which includes NSW law enforcement, government and other bodies, is currently considering these issues.[44] There was no evidence as to the timeframe for this work.

---

41 AGD, *Supplementary Submission 44.2*, p.3.

42 NSW Government, *Submission 49*, p.6.

43 AGD, *Supplementary Submission 44.2*, p.7.

44 AGD, *Supplementary Submission 44.2*, p.7.

Admissibility of Evidence

6.39 The AFP also identified the need to demonstrate the chain of handling of digital evidence and the lack of uniformity in evidence laws across Australian jurisdictions as two challenges to the admission of digital evidence in Australian courts. In particular, the ability to store, review and analyse voluminous data and a lack of tools/systems to 'robustly demonstrate chain of evidence handling of digital media' was an issue from a law enforcement point of view.[45]

6.40 The AGD agreed that practical handling of large volumes of complex material takes time and resources to conduct the necessary analysis. The analysis and presentation of digital evidence in court is made more complex if it has been subject to encryption.[46] Nevertheless, cyber crime, like other forms of crime must be established by admissible evidence. The AGD said:

> This includes proving continuity of digital evidence by presenting evidence of the chain of handling. Such evidence may be detailed given the involvement, for example, of computer forensic analysts, but this forms a necessary part of proving matters before criminal courts.[47]

6.41 In relation to uniform evidence law, the AGD advised that the Commonwealth, NSW, Victoria, Tasmania the ACT and Norfolk Island have adopted a harmonised approach under the Uniform Evidence Acts regime developed through the Standing Committee of Attorneys-General (SCAG).[48] The Department said that SCAG has an ongoing role in the harmonisation of evidence law.[49] There was no assessment of the status of that work or the likelihood of achieving uniformity in the near future.

Foreign business records

6.42 The NSW Police raised concern about the admissibility of records from, for example, Microsoft and Gmail, which are classed as 'business records'. It was suggested that such evidence should be admissible by 'information and belief' only rather than strict proof. Part 3 of the *Foreign Evidence Act 1993* (Cth) provides a means of adducing foreign evidence obtained through mutual assistance in Australian criminal proceedings. The AGD

45 AFP, *Supplementary Submission 25.1,* pp.9-10.
46 AGD, *Supplementary Submission 44.2*, p.7.
47 AGD, *Supplementary Submission 44.2*, p.7.
48 AGD, *Supplementary Submission 44.2*, p.7.
49 AGD, *Supplementary Submission 44.2*, p.7.

advised the Committee that amendments to that Act, currently before the Senate, would provide more flexibility in the testimony requirements but it will not go so far as to only require admission on the basis of the 'information and belief' of a law enforcement officer.[50]

6.43 The Department stressed the importance of preserving 'an appropriate balance' between individual rights and sufficient legal and judicial flexibility to secure international crime cooperation. The Department also said that its International Crime Cooperation Central Authority is experienced in working closely with the US Department of Justice to ensure evidence obtained from ISPs complies with the requirements for admission in Australian proceedings.[51]

International Cooperation

6.44 In the context of international cooperation, the AFP's evidence highlighted two particular issues:

- lack of timely access to evidence to identify offenders and for court proceedings; and
- inconsistent legislation in different countries that undermine investigative methods and prevent extradition and prosecution.[52]

6.45 AusCERT emphasised the importance when dealing with cyber crime for LEAs to be able to quickly secure digital evidence, often in multiple jurisdictions, to ensure that it is retained and the forensic quality of the evidence is preserved.[53] However, the AFP noted that getting information for forensic analysis from overseas ISPs and telecommunication services is often too slow to indentify an offender. Data is generally not received in time to be submitted to court and, in some cases, has taken up to eighteen months unless the investigation is high profile. Much of the international cooperation is done on a police to police basis because the formal mutual assistance regime is slow and makes it difficult to obtain evidence to identify offenders fast enough to enable a prosecution.[54]

6.46 Inconsistent legislation across countries can also mean that LEAs methods are sometimes thwarted. For example, inconsistent telecommunications intercept data retention laws can mean that evidence that would be

50 Foreign Evidence Amendment Bill 2008; AGD, *Supplementary Submission 44.2*, p.8.

51 AGD, *Supplementary Submission 44.2*, p.8

52 AFP, *Supplementary Submission 25.1*, pp.8-9.

53 AusCERT, *Submission 30*, p.15.

54 AFP, *Supplementary Submission 25.1,* pp.8-9.

available in Australia is not available where the service or data holdings are based in a foreign country.[55]

6.47 Inconsistent legislation or a lack of cyber crime offences can also mean that individuals based overseas escape extradition and prosecution for cyber offences because there is no similar offence in the country of origin (double criminality test).[56]

6.48 According to AGD the government to government processes for mutual assistance in criminal matters can take:

> … from a few days or weeks in very urgent or less complex cases, to several months or years in cases which require the collection of extensive material, or which relate to complex investigations. In contrast, requests for police-to-police assistance can sometimes be acted on much more quickly.[57]

6.49 The AGD told the Committee that Australia is already a party to approximately 25 bilateral treaties on mutual assistance in criminal matters.[58] Further, a comprehensive review of Australia's mutual assistance legal regime was completed recently and an exposure draft of the Extradition and Mutual Assistance in Criminal Matters Legislation Amendment Bill released for public consultation in July 2009:

> A key intent of the reforms in this Bill is to streamline and modernise Australia's laws to ensure the mutual assistance regime is able to respond to advances in technology.[59]

6.50 Some of the proposed reforms include:

- provision for a warrant to covertly access stored communications (such as email records) for foreign law enforcement purposes; and
- allow the disclosure of existing data, such as subscriber details and call charge records without the need for a formal request from the foreign country (i.e. on a police to police basis).[60]

6.51 The draft exposure Bill was said to contribute to Australia's ability to meet Convention obligations and the Department is assessing whether any

---

55 AFP, *Supplementary Submission 25.1,* pp.8-9.
56 AFP, *Supplementary Submission 25.1*, pp.8-9.
57 AGD, *Supplementary Submission, 44.2*, p.4.
58 AGD, *Supplementary Submission 44.2*, p.4.
59 AGD, *Supplementary Submission, 44.2*, p.5.
60 AGD, *Supplementary Submission, 44.2*, p.5.

additional changes are needed to meet the international cooperation obligations.[61]

6.52 In addition to these reforms, AGD agreed that participation in the Council of Europe Convention on Cybercrime would increase Australia's ability:

> … to obtain international assistance from other parties to the Convention in investigating potential cyber crime offences, particularly in relation to accessing telecommunications.[62]

6.53 The Council of Europe Convention on Cybercrime is discussed below.

Committee View

6.54 The evidence indicated that there has been a considerable expansion in police powers to ensure that LEAs are able to adapt investigative methods to the high tech environment. There appears to be an ongoing program of legal policy development in response to problems as they are identified. Some of those reforms (identity fraud, foreign business records) were before the Parliament during this inquiry. Reform of the mutual assistance regime to respond to new technology was released for public consultation in July 2009. These measures go some way to strengthening law enforcement capability in relation to high tech crime.

6.55 However, the Committee is concerned that many Australian ISPs and telecommunications carriers appear to be unable to meet their statutory obligations under the TIA Act. The role and responsibilities of ISPs are discussed in the next chapter, where it is noted there are between 500-600 ISPs currently in operation in Australia alone. This problem is magnified when dealing with ISPs overseas, especially where the laws on the retention of data vary.

International Legal Framework

6.56 As has been noted throughout this report, a significant portion of cyber crime experienced by Australians originates from overseas. This makes international cooperation critical to efforts to criminalise, detect, disrupt, prevent, and ultimately to pursue effective law enforcement action.[63]

---

61 AGD, *Supplementary Submission, 44.2*, p.5.

62 AGD, *Supplementary Submission, 44.2*, p.4.

63 Internet Safety Institute, *Submission 37*, p.7; Microsoft Australia, *Submission 35*, p.1.

6.57 The UN International Telecommunications Union (ITU) is active on the issue of cyber crime but there is no UN sponsored international treaty dedicated to this specific subject matter. The Australian Bankers Association (ABA) advocated a more proactive stance by Australia in international fora for the development of an international legal regime targeting cyber crime.[64]

6.58 In particular, it argued for a review and, if necessary, an extension of the existing UN Convention on Transnational Organised Crime (and relevant bilateral agreements), to address the problem of cyber crime. The ABA also expressed concerns about the adequacy of the implementation of that treaty, including in the area of mutual legal assistance.[65]

Council of Europe Convention on Cybercrime

6.59 The most relevant international treaty on this subject is the Council of Europe Convention on Cybercrime (the Convention), which is designed to promote the harmonisation of national laws on cyber crime and to aid international law enforcement cooperation.[66]

6.60 Mr Alexander Seger, Head of the Economic Crime Division, Council of Europe informed the Committee that, although the Convention was developed by the Council of Europe, it was designed to have global scope and Non-member States of the Council of Europe have been encouraged to sign and ratify the treaty.[67] The USA, Canada, Japan and South Africa participated in the treaty's preparation and have signed, and in the case of the USA, have ratified the treaty:

> By the end of June 2009, 26 countries were full parties to the Convention, while an additional 20 had signed it and another 5 had been invited to accede. A further 50 to 70 countries are using the Convention as a guide and have or are in the process of adapting their cybercrime legislation along the lines of this treaty.[68]

---

64 ABA, *Submission 7*, pp.9-12.

65 ABA, *Submission 7*, pp.9-12.

66 Convention on Cybercrime, European Treaty Series No.185 (opened for signature Budapest 23.11.2001 entered into force 1.7.2004).

67 Directorate General of Human Rights and Legal Affairs, Council of Europe, *Submission 31*, p.3.

68 Council of Europe, *Submission 31*, p.3; at the time of writing 27 countries had signed and ratified or acceded to the treaty and 19 had signed the treaty but not yet proceeded to ratification, viewed 11 March 2010, <http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=1&DF=11/03/2010&CL=ENG>.

6.61 Any country can seek accession and then be invited to accede. Chile, Costa Rica, the Dominican Republic, Mexico and the Philippines have been invited to accede and it is expected that by the time of accession these countries will have harmonised their national law with the Convention.[69]

6.62 Several witnesses urged the Committee to recommend that the Australian Government seek accession to the Convention.[70] The Council of Europe emphasised that efficient international cooperation is crucial to combat cyber crime and to secure evidence on computer systems:

> For that reason, the Convention contains a range of general and specific measures to facilitate cooperation and allow the use of domestic measures (such as the expedited preservation) also in relation to international cooperation.[71]

6.63 To support the implementation of treaty obligations, the Council of Europe has produced Guidelines for the Cooperation between Law Enforcement and Internet Service Providers against Cybercrime.[72]

6.64 The Council of Europe also pointed out a number of other benefits including the ability of States parties to participate in the Cybercrime Convention Committee, which monitors treaty implementation and initiates future work, such as the elaboration of additional protocols.[73] Australia's accession to the treaty would also serve as a positive example to other countries in the Asia Pacific region.[74]

6.65 In preliminary comments on Australian law, the Council of Europe observed that substantive offences appear to be already covered:

> …although – perhaps due to the specifities of the Australian legal system – a different approach seems to have been followed for some of them. For example, in some Australian legal provisions different types of conduct listed in the Convention have been combined (e.g. illegal access, data interference, system interference) or individual provisions of the Convention are reflected in several different provisions in Australia. This is

---

69 Council of Europe, *Submission 31*, p.3.

70 Microsoft Australia, *Submission 35*, p.9; Queensland Government, *Submission 67*, p.7; AIIA, *Submission 22*, p.3; AusCERT, *Submission 30*, p. 15.

71 Council of Europe, *Submission 31*, p.4.

72 Project Cybercrime, viewed 23 March 2010 <www.coe.int/cybercrime>. Adopted by the Global Conference Cooperation against Cybercrime, Council of Europe, Strasbourg, 1-2 April 2008.

73 Council of Europe, *Submission 31*, p.5.

74 Council of Europe, *Submission 31*, p.5

> compatible with the Convention but may create difficulties in international cooperation when applying dual criminality.[75]

6.66 In relation to procedural law and practice the Council of Europe commented that:

> …it seems that some tools (search and seizure, production order etc) are available, while others are not (e.g. expedited preservation).[76]

6.67 The AGD told the Committee that Australia is already compliant with some obligations contained in the Convention but:

> There remain a number of complex issues that the Government will need to consider, some of which may require significant legislative amendment. The Australian Government is currently reviewing existing domestic legislation to identify what action may be necessary to implement the Convention in Australia's domestic law, should it decide to become a party to the Convention.[77]

6.68 Specifically, the AFP suggested that some amendments to the *Telecommunications (Interception and Access) Act 1979* (TIA Act) may be necessary.[78] The Committee noted, for example, that intercept material obtained by police under the TIA Act cannot be shared with foreign countries.[79]

6.69 The Council of Europe offered its assistance in conducting a detailed analysis to assess whether Australian legislation and practice is fully in line with the Convention.[80] Microsoft Australia also provided the Committee with a study of computer security, privacy, spam and online child safety laws in 14 countries across the Asia Pacific Region. The study included analysis of Australian cyber crime laws benchmarked against the Convention.[81]

---

75 Council of Europe, *Submission 31*, p.4.

76 Council of Europe, *Submission 31*, p.4.

77 AGD, *Submission 44*, p.14.

78 AFP, *Transcript of Evidence,* 9 September 2009, p.11.

79 Section 13A of the *Mutual Assistance in Criminal Matters Act 1987* (Cth) expressly excludes material obtained under the TIA from being provided to a requesting foreign country to assist in an investigation or proceedings for a serious offences against that country's domestic law.

80 Council of Europe, *Submission 31*, p.4.

81 Microsoft Australia, *Submission 35,* pp. 6-10; Microsoft Corporation Ltd, *Asia Pacific Legislative Analysis: Current and Pending Online Safety and Cybercrime Laws: A Study by Microsoft*, November 2007, viewed 10 March 2010, <www.microsoft.com/asia>.

6.70 The study found there was a strong alignment of Australia's current cyber crime framework with the Convention's 'core offences' of data interference; computer related forgery and fraud offences; and corporate criminal liability for cyber crime.[82] However, it found that there is scope to strengthen provisions on illegal access, system interference and misuse of device offences.[83] Specifically, Microsoft Australia said:

> The Code's unauthorised access offence only applies in respect of data that is protected by an access control system (this qualification is permitted by the Convention).
>
> The Code's data interference offence is likely to regulate a broader range of conduct than its Convention counterpart due to its application to reckless data interference as well as that caused intentionally.
>
> …
>
> The Code does not contain an equivalent to the Convention's system interference offence, but its unauthorised impairment of electronic communications offence is targeted at denial of service attacks in the same way that the Convention system interference offence is (at least in part).[84]

6.71 Finally, in respect of producing, supplying, possessing or procuring data (which is defined as including computer programs) with intent to commit a computer security offence, Microsoft said these 'are best viewed as a partial implementation of the Convention's misuse of devices offence'.[85]

6.72 Overall, however, Microsoft Australia concluded that:

> … Australia has demonstrated a solid commitment to robust legislation, but could further strengthen some of these provisions in closer alignment with the Cybercrime Convention. Australia has already been playing an important role in achieving regional and global consistency. It is effectively functioning as a policy bellwether for the region.[86]

6.73 Finally, the Cyber Space Law and Policy Centre (CLPC) pointed out that some of the special evidence gathering obligations of the Convention raise significant privacy issues. As Australia does not have a domestic Charter

82 Microsoft Australia, *Submission 35*, p.7.
83 Microsoft Australia, *Submission 35*, p.7.
84 Microsoft Australia, *Submission 35*, p.8.
85 Microsoft Australia, *Submission 35*, p.7.
86 Microsoft Australia, *Submission 35*, p.8.

of Rights and Freedoms against which such provisions can be independently assessed, the CLPC advised that these provisions should be subject to careful scrutiny before being implemented in Australia.[87]

Committee View

6.74 The transnational nature of cyber crime and the importance of consistency in both the substantive offences and procedural law to strengthen international cooperation make the review and, if necessary, amendment of Australian laws an important priority for all Australian governments. The Convention was finalised in 2001 and entered into force in 2004. At the time of writing in 2010, 46 countries had either signed or signed and acceded or ratified the Convention, including the USA, Australia's major partner in fighting transnational cyber crime.

6.75 The majority of evidence to the Committee indicates that Australian law is already substantially aligned with the offence provisions and some procedural aspects of the Convention. However, the Committee is concerned that Australia's progress has been too slow and is disappointed that AGD's evidence lacked a clear framework for action and specific timetable for seeking accession to the Convention.

6.76 There is general agreement that Australians are benefitting from the high level of ICT penetration into the Australian economy and increasing IT literacy across the community. In light of the importance of ICTs, the Committee believes that Australia governments should give priority to finalising the internal review and necessary reforms and move expeditiously toward seeking accession to the Convention. The shaping of Australian law to comply with the Convention should also take into account Australia's existing obligations under the International Covenant on Civil and Political Rights.

6.77 Overall, however, the Committee believes that Australia's participation will strengthen international law enforcement cooperation and enable Australia to participate in future treaty development and influence global legal regimes. Participation in the treaty will also support Australia's work in other international fora and the Asia Pacific Region.

87 CLPC, *Submission 62.1*, p.3.

Recommendation 9

That the Federal Attorney-General, in consultation with State and Territory counterparts, give priority to the review of Australian law and practice and move expeditiously to accede to the Council of Europe Convention on Cybercrime.

Tackling Botnets

6.78 There is wide agreement among police, researchers, IT security companies and governments around the world that botnets are the key tool for the commission of cyber crime:

> Botnets are said to be involved in most forms of cybercrime and civil wrong ranging from sending spam, to denial of service attacks, to child pornography distribution, to worm propagation, to click fraud, to keylogging technology and traffic sniffing which captures passwords and credit card information, and to mass identity theft.[88]

6.79 Similarly, Microsoft Australia emphasised that:

> As online criminals increasingly access and control protected networks of computers remotely and without authorisation, creating "botnets" of literally hundreds of thousands of machines that are used to attack other machines, perpetrate identity theft, spread spyware and malware, or disrupt Internet functions, more needs to be done to identify, stop and prosecute these criminals ("botherders").[89]

6.80 The IIA argued that since the passage of the *Cybercrime Act 2001* cyber crime has become more sophisticated and moved from one-off events to organised crime on an industrial scale. Cyber crime now relies on thousands of infected home computers exposing more general weaknesses in the current regime.[90] From IIA's perspective the problem is not the lack of a legal framework but the inability of traditional institutions to respond to the complexity of cyber crime. It was argued that tackling botnets

88 CLPC, *Submission 62*, p.3; Rychlicki T., *Legal Issues of Criminal Acts Committed Via Botnets* (2006) Computer and Telecommunications Law Review 12 (5), p.163 as cited CLPC, *Submission 62*, p.3.

89 Microsoft Australia, *Submission 35*, p.

90 For example, IIA, *Submission 54*, p.2.

requires a more concerted effort, and the lack of prosecutions and light sentences has contributed to a lack of community awareness of the problem.[91]

6.81 The IIA were not alone in this view. The CLPC, Microsoft and Sophos also stressed the importance of tackling the botnet infrastructure, by identifying and neutralising botnets and targeting botnet herders.[92]

6.82 As noted in Chapter 5, the CLPC was critical that law enforcement strategy puts little emphasis on prosecuting botherders or addressing botnets run by organised crime.[93] The CLPC said that 'cyber crime policy should place a significant emphasis on the disruption and dismantling of botnets, as opposed to the mere prosecution of botnet herders'.[94]

6.83 In one case, the AFP identified distributed denial of service attacks committed by botnets containing more than 100,000 compromised computers across more than 120 countries:

> …the ability of law enforcement to investigate and prosecute individuals behind such attacks is often thwarted by the transnational nature of the Botnet make up and control systems.[95]

6.84 The Committee was also told that to prosecute a person running a botnet the police would need statements from potentially thousands of individuals that the perpetrator did not have authority to enter and operate their computer.[96] However, AGD disagreed and told the Committee that the Commonwealth Director of Public Prosecutions is able to prosecute on the basis of representative charges, which establish a course of conduct by the defendant together with forensic evidence to show how the botnet operated.[97]

6.85 Fujitsu told the Committee, that in their view, there are gaps in the law and policy that would support a more strategic approach. For example:

- insufficient legislation that targets the criminal underground economy, the people involved, and the tools they use to write malware;
- restrictions on the deployment of tools to identify suspects; and

---

91 IIA, *Submission 54*, p.5.

92 See CLPC, *Submission 62*; Microsoft Australia, *Submission 35*; Sophos, *Submission 66*.

93 CLPC, *Submission 62*, p.3.

94 CLPC, *Submission 62*, p.3.

95 AFP, *Submission 25,* p.9.

96 AFP, *Supplementary Submission 25.1,* pp. 9-10.

97 AGD, *Supplementary Submission 44.2,* p.8.

- lack of legislation that allows law enforcement or other entities to deploy technical capability to remove virus/trojans/malware from victims.[98]

6.86 David Jones, ThreatMetrix Pty Ltd also argued for a fresh look at cyber crime laws to better respond to the current environment of botnets and compromised hosts.[99]

6.87 In response to a question from the Committee about the ability to conduct network wide strategies, the AGD advised that existing Criminal Code Part 10.7 computer offences would be violated if an anti-malware program intended to disinfect PCs were released to combat a widely distributed virus.[100]

Committee View

6.88 Since the introduction of computer offences the problem of cyber crime has moved onto an industrial scale organised through loose networks. There was a clear message that the IT security companies are unable to entirely protect their customers and traditional law enforcement methods are unlikely to get on top of this problem. Legal policy and law enforcement strategy also needs to:

- target the underground cyber crime economy;
- target the botherders;
- tackle botnets through disruption; and
- remediate compromised computers (See Chapter 7).

6.89 The Committee noted concerns that police lack sufficient tools to identify offenders or deploy technical capability to remove malicious software. In the Committee's view, Australian LEAs must have the tools needed to work with international partners in a concerted effort to tackle the botnet problem and prosecute the members and leaders of organised criminal networks.

98 Fujitsu, *Submission 13*, p.7.

99 ThreatMetrix Pty Ltd, *Submission 19*, p.14.

100 AGD, *Supplementary Submission 44.2*, p.2.

Recommendation 10

That Australia's cyber crime policy strategically target the underground economy in malicious IT tools and personal financial information; the disruption of botnets and the identification and prosecution of botherders .

Future Initiatives

6.90 The NSW Government argued that, while it had introduced specific computer and identity crime offences, this should 'only be the beginning of legislative reforms to tackle cyber crime'.[101] In particular, NSW argued that the computer offences are 'focused on the hardware rather than cyberspace more generally' and the identity crime offences are aimed at the members of syndicates rather than the head of those organisations/networks that develop the means to obtain the information.[102]

6.91 To maintain a coordinated and ongoing legislative reform effort, the NSW Government recommended that a national cyber crime working group be established to develop legislative initiatives for cyber crime for both Commonwealth and State jurisdictions to implement.[103] The working group would report to the appropriate Ministerial Council. It was suggested that this group could also give further consideration as to whether Australia should become a signatory to the Council of Europe Convention on Cybercrime. From NSW's perspective, the group should include a cross section of policy staff from justice and law enforcement agencies, including significant input from the AFP High Tech Crime Operations Centre.[104]

Committee View

6.92 There does not appear to be any existing dedicated cross jurisdictional working group on cyber crime, although the Commonwealth may consult on specific initiatives. Many issues would be dealt with via the Model Criminal Code Officers Committee, which reports to SCAG. As noted

101 NSW Government, *Submission 49*, p.5.
102 NSW Government, *Submission 49,* p.5.
103 NSW Government, *Submission 49*, p.6.
104 NSW Government, *Submission 49*, p.6.

above, the Committee is satisfied there have been significant reforms in this area.

6.93 However, there is a need to remain responsive to the evolving nature of cyber crime. Consequently, the Committee sees some merit in a specialist working group dedicated to cyber crime that can be focused and responsive. In particular, this group should put a high priority on facilitating international cooperation in the investigation of organised criminal networks and the problem of botnets.

Recommendation 11

That the Commonwealth, State and Territory governments establish a national working group on cyber crime to maintain an ongoing, dedicated mechanism for the review and development of legislative responses to cyber crime.

That the working group take a whole of cyberspace perspective and consider relevant IT industry, consumer protection and privacy issues as well as the criminal law.