5

Domestic and International Coordination

Introduction

5.1 This chapter gives a broad outline of the national framework for coordinating cyber crime policy and existing mechanisms for international engagement.

5.2 The chapter concludes that existing coordination mechanisms are heavily weighted toward national security and critical infrastructure. A more centralised and genuinely national approach is required to ensure that strategic responses to cyber crime that impact on the broader Australian society are as effective as possible.

Cyber Security Strategy

5.1 Since 2001 the Australian Government's approach to e-security has been governed by the *E Security National Agenda.* The policy was reviewed in 2004 and 2006. In 2008 a further review was initiated in response to the 'increased level of cyber threat' and rapid growth in the use of information and communication technology, including the roll out of the National Broadband Network.[1] On 23 November 2009 the *Cyber Security Strategy* was launched bringing together a number of existing e-security activities under the umbrella of one policy and introducing some new initiatives.[2]

[1] AGD, *Submission 44*, p.6.

[2] Attorney General Hon Robert McClelland MP; Minister for Broadband, Communications and the Digital Economy, Senator The Hon Stephen Conroy; Minister for Defence, Senator the Hon John Faulkner, Joint Media Release, *Australian Cyber Security Strategy Launched*, 23 November 2009; *Cyber Security Strategy,* Australian Government, p.vi.

5.2 The *Cyber Security Strategy* emphasises the protection of national security, government computer systems and critical infrastructure. There will be a benefit to the public through the increased capacity to protect government computer systems and institutions, such as banks, and public utilities on which the whole community rely. However, the new computer response team, CERT Australia, does not receive complaints about cyber crime or providing technical assistance to the general public or small and medium sized businesses.

5.3 In practice, the *Cyber Security Strategy* retains the previous emphasis on community education so that end users can better protect themselves against online crime. The Committee was told that community education alone is no longer a sufficient response to sophisticated cyber crime activities that impact the whole community. It was argued that there needs to be more importance attached to the needs of consumers and business generally and more strategic approaches to the inter-connected nature of cyber space.[3]

Domestic Policy Coordination

5.4 Under the current arrangements, the Attorney-General's Department (AGD) has primary responsibility for e-security policy across the Australian Government and is the lead agency for identity security and critical infrastructure.[4] The Committee was told that the E-Security Policy and Coordination Committee (ESPaC), a bi monthly interdepartmental committee chaired by AGD, provides a whole of government perspective on e-security policy and coordination.[5]

5.5 Following the *E Security Review* the Committee has been renamed the Cyber Security Policy and Coordination Committee and its membership has been expanded. Membership is now comprised of the:

- Australian Federal Police (High Tech Crime Operations);
- Australian Government Information Management Office;
- Australian Security Intelligence Organisation;
- Defence Signals Directorate;

[3] Mr Graham Ingram, AusCERT, *Transcript of Evidence*, 11 September 2009, p.4; Cyber Space Law and Policy Centre, *Submission 62*, p.6.

[4] AGD, *Submission 44*, p.2.

[5] AGD, *Submission 44*, p.7

- Department of Broadband, Communications and the Digital Economy (DBCDE);
- Department of Defence; and
- Department of the Prime Minister and Cabinet (PM&C).

5.6 The Cyber Security Policy and Coordination Committee:

- provides whole of government strategic leadership on cyber security;
- determines priorities for the Australian Government;
- coordinates the response to cyber security events; and
- coordinates Australian government cyber security policy internationally.[6]

5.7 The Committee formally reports on the progress of its annual work plan to the Deputy National Security Advisor on an annual basis. The Committee also coordinates the 'provision of threat and security environment assessments to the National Security Committee of Cabinet, through the Secretaries Committee on National Security as required'.[7]

National Coordination of Cyber Space Policy

5.8 The evidence demonstrated that Internet activity involves a range of policy areas, including criminal law, privacy, consumer protection, telecommunications, broadcasting, and corporation law. Consequently, there is a plethora of Commonwealth, State and Territory departments and agencies with responsibility for some aspect of the wider problem of cyber crime.

5.9 In relation to policy, AGD has responsibility for criminal law and law enforcement policy but it does not have policy responsibility for cyber safety, privacy or consumer protection.[8] These areas fall variously to DBCDE, PM&C, and Treasury. State and Territory Governments are also responsible for a range of legal policy in criminal law, privacy, education, and consumer protection that impact on cyber crime.

5.10 Federal, State and Territory police forces enforce the laws against cyber crime. In addition, a range of civil regulatory bodies have an enforcement role in relation to different aspects of cyber crime activity:

[6] *Cyber Security Strategy*, Australian Government, 2009, p.30.

[7] AGD, *Submission 44*, pp. 22-23.

[8] AGD, *Submission 44*, p.14.

- Australian Communications and Media Authority (ACMA) administers the Australian Internet Security Initiative (botnet detection) and administers the *Spam Act 2003* (Cth);
- the Australian Competition and Consumer Commission (ACCC) hosts the *ScamWatch* website, and takes thousands of complaints of online fraud and scams, which it deals with in the context of misleading and deceptive trade under the *Trade Practices Act 1974* (Cth);
- State and Territory Fair Trade offices deal with these matters under State and Territory law;
- the Federal Privacy Commissioner administers the *Privacy Act 1988* (Cth), which regulates the collection and disclosure of personal information;
- complementary privacy laws are administered by State and Territory Commissioners; and
- corporations are regulated by the Australian Securities and Investment Commission (ASIC) under the *Australian Securities and Investments Commissions Act 2001* (Cth) and the *Corporations Act 200* (Cth).

5.11 Although difficult to avoid, this highly decentralised approach was regarded by some as an impediment to a nationally coordinated and strategic response to tackling the problem of cyber crime. For example, Mr Alastair MacGibbon, Director Internet Safety Institute said:

> … there no single institution in Australia (or for that matter anywhere else in the world) which has a whole-of-internet national view of eSecurity victimisation.[9]

5.12 The Cyber Space Law and Policy Centre (CLPC) said that as a consequence of this fragmentation legal policy and regulatory measures are 'convoluted' and unable to target the interlinked nature of cyber crime and its related activities.[10] The witness doubted whether Australian law could effectively deal with the commission of cyber crimes facilitated through a mix of these activities because 'each one is categorised and dealt with by separate agencies (police, ACMA, and the ACCC) making investigation difficult or impossible'.[11]

[9] Internet Safety Institute, *Submission 37*, p.11.

[10] CLPC, *Supplementary Submission 62.1*, p.5.

[11] CLPC, *Supplementary Submission 62.1*, p.5.

5.13 Microsoft advocated that Australia consider a more expansive strategy and create a 'cyber Tzar' position located in PM & C and a strategy that engages 'all elements of national power':

> When one recognises the breadth of the challenge and the need for a massively decentralised but coordinated response among the federal, state and territory agencies, we believe that the Committee should consider whether or not Australia's national cyber security strategy and its implementation should be led by a single coordinating authority at the highest Executive level, like the Department of Prime Minister and Cabinet or through an appointed "cyber security czar". As the Committee would be aware, the US is moving to a similar model, where their national cyber security strategy will be led and coordinated by the White House.[12]

5.14 Mr James Shaw, Director, Government Relations, Telstra Corporation Ltd., also advocated a centralised point within government to manage a more coordinated approach:

> At the moment it is dealt with in a variety of areas of government. In their best endeavours they collaborate as best they can. A lot of that, though, is ad doc rather than done in a strategic sense from one point in government with an overall policy strategy agenda.[13]

5.15 To expand the reach of Australia's e-security strategy, Telstra suggested the creation of a National Cyber Crime Advisory Committee 'focussing on strategic leadership and information sharing between public and private sectors, federal, state and local entities'.[14] Such a Committee would comprise independent experts from a range of cyber space related areas, including consumers, to provide best advice on a range of cyber crime issues.[15]

5.16 The Australian Communications Consumer Action Network (ACCAN), also highlighted the need for a 'more coordinated and rigorous approach' to protecting online consumers.[16] It was suggested that Australia should adopt a similar approach to that of the UK and create an Office of Online Security, which can address the 'multitude of economic and social

[12] Microsoft Australia, *Submission 35*, p.6.

[13] Mr James Shaw, Telstra Corporation Ltd., *Transcript of Evidence*, 11 September 2009, pp.44-45.

[14] Telstra Corporation Ltd, *Submission 43*, p.3.

[15] Mr James Shaw, Telstra Corporation Ltd., *Transcript of Evidence*, 11 September 2009, p.44.

[16] ACCAN, *Submission 57*, p.1.

implications of online security issues'.[17] The UK Office of Cyber Security operates within the Cabinet Office to provide strategic oversight.

5.17 ACCAN suggested that an Australian Office of Online Security should have responsibility for high level policy on cyber security and its impact on consumers, and report at 'Cabinet level on improvements, research and further challenges in cyber security.'[18] The Office could, for example, set benchmarks for preinstalled security features for the sale of computers and work with DBCDE to develop a National Strategy for E-Security Awareness.

5.18 Mr Graham Ingram, Director, AusCERT, advocated a 'cyber space' perspective that integrates the relevant government agencies and clearly identifies the role and responsibilities of ISPs, Domain Name Registrars, and IT companies. He proposed that that these private stakeholders should all be part of a nationally coordinated effort to reduce e-security risks.[19] Similarly, Mr Alastair MacGibbon, Director, Internet Safety Institute, also suggested that private companies, such as ISPs and Domain Name Registrars, have some responsibilities in this area.[20]

5.19 The whole Internet community needs to be brought together:

> We need to have a national response, the same way as if we have a response to a pandemic. We need everyone to know what they are doing and having it coordinated. We do not have that strategic approach to this problem currently.[21]

5.20 Sophos also advocated a more holistic national approach that involves IT vendors, and ISPs in a concerted effort to deal with the problem of botnets:

> With suitable Federal legislation, with mandated remediation or suspension, with national education initiatives, and with appropriate resources within government and ISPs, it would be possible to place additional pressure on these hijacked computers to be cleaned up. If successful, this would reduce the number of Australian-based bots, benefiting internet users not just in Australia, but all over the world.[22]

[17] ACCAN, *Submission 57*, p.5.

[18] ACCAN, *Submission 57*, p.5.

[19] AusCERT, *Submission 30*, pp. 14 and 17; see also, *Transcript of Evidence,* 11 September 2009, p.5.

[20] Mr Alastair MacGibbon, *Transcript of Evidence*, 11 September 2009, pp.60-61.

[21] Mr Graham Ingram, AusCERT, *Transcript of Evidence*, 11 September 2009, p.5.

[22] Sophos, *Submission 66,* p.6.

5.21 The role and responsibilities of ISPs and Domain Name Registrars and Resellers is discussed in Chapter 7.

Committee View

5.22 The Australian community's increasing reliance on ICT and the Internet combined with the complexity of online crime poses a significant challenge to policy makers, law enforcement and regulatory authorities. As discussed in Chapter 2, the interconnectedness of cyber space means that both the legitimate and illegitimate use of these technologies crosses inter-state and international boundaries and blurs the distinctions between civil and criminal matters.

5.23 This has implications for the development of a nationally coordinated and integrated policy on cyber security, strategic approaches to legal regulation, and the development of systems that maximise expertise and resources. The Committee commends the efforts of regulators and agencies tackling the problems of malicious Internet use but notes that the system remains inherently complex and fragmented.

5.24 The current *Cyber Security Strategy* places significant emphasis on national security and the protection of critical infrastructure. These are important national objectives. However, the Committee is concerned that education and awareness raising is no longer sufficient on its own as a national strategic response to the problem of cyber crime that impacts on the wider Australian community.

5.25 The breadth and complexity of the problem justifies a more national and centrally coordinated strategy that takes a more comprehensive and integrated cyber space perspective.

Recommendation 3

That the Australian Government establish an Office of Online Security headed by a Cyber Security Coordinator with expertise in cyber crime and e-security located in the Department of Prime Minster and Cabinet, with responsibility for whole of Government coordination. The Office is to take a national perspective and work with State and Territory governments, as well as federal regulators, departments, industry and consumers.

That the Australian Government establish a National Cyber Crime Advisory Committee with representation from both the public and private sector to provide expert advice to Government.

International Engagement

5.26 The DBCDE submitted that:

> Given the borderless nature of the internet, the isolated efforts of individual countries are not enough to effectively address global e-security challenges. Australia is actively working bilaterally and in key international forums to improve the international e-security environment. The main objective of this work is to assist countries that may be sources of e-security threats to improve their domestic response and to set in place international cooperative arrangements to address e-security threats.[23]

5.27 Similarly, the AGD outlined the importance of international engagement to promote coordinated international policy development, information sharing on cyber crime trends and response preparedness.[24]

5.28 The Departments identified a significant number of international fora in which Australia participates in and, in some cases, takes a leading role:

- **International Watch and Warning Network (IWWN)** is an international forum for international cooperation and coordination on cyber information sharing and incident response. It is comprised of government cyber security policy makers, managers of computer

[23] DBCDE, *Submission 34*, p.15.

[24] AGD, *Submission 44*, p.13.

security incident response teams with national responsibility and law enforcement representatives with responsibility for cyber crime matters.

- **Asia-Pacific Economic Cooperation Telecommunications and Information Working Group (APEC TEL)** aims to improve telecommunications and information infrastructure in the Asia-Pacific region by developing and implementing appropriate telecommunications and information policies.
- The DBCDE submitted that Australia is a key driver of e-security work in the APEC group and has led a number of projects including:
  - ⇒ development of awareness raising materials for small business and consumers on wireless security and Voice Over Internet Protocol (VoIP) security;
  - ⇒ a joint project with the United States within APEC TEL on e-security awareness raising which aims to develop a coordinated approach in the region;
  - ⇒ participating actively in projects focused on ICT products and standards and hand-held mobile device security; and
  - ⇒ joint projects between APEC TEL and the OECD on e-security issues. The two groups have developed an analytical report on malware. These projects ensure common policy approaches are developed over a wider number of countries which leads to better outcomes for consumers.
- **Meridian** process brings together senior government officials from around the world who are policy makers on issues of critical information infrastructure protection (CIIP).
- **International Telecommunication Union (ITU)** is the leading United Nations agency for information and communication technologies and is currently examining a range of e-security issues under its Global Cybersecurity Agenda. The ITU's powers can bind member countries to take specific courses of action.
  - ⇒ The DBCDE participated in the regional workshop on *Frameworks for cybersecurity and critical information infrastructure protection* in August 2007 in Vietnam. This representation has allowed Australia to play a part in the development of policy documents on these issues for developing countries.
  - ⇒ The DBCDE held an ITU workshop on e-security and critical infrastructure protection in Brisbane in July 2008. This provided Australia with an opportunity to bring together Pacific Island countries to share e-security experiences and resources with these countries.

- ⇒ The ITU, with assistance from the Department, commissioned a scoping study on the feasibility of establishing a Computer Emergency Response Team for the Pacific Region (PacCERT). The first part of the study identified a definite need to develop a PacCERT, and found that a growing capability to deliver this already exists within the region. The second part of the study, relating to the implementation of a PacCERT, was to be finalised by the ITU in the second half of 2009. This work will include a detailed project plan covering staffing, location, funding, governance and the required linkages with other relevant parties, including domestic law enforcement authorities.

- **OECD Working Party for Information Security and Privacy (WPISP)** provides a platform for pursuing international aspects of Australian communications policy relating to cyber security, critical infrastructure protection, authentication, privacy, malware and spam.
  - ⇒ Australia currently chairs this Working Party and has been an active contributor in the development of common policy approaches to identity management, malware, critical infrastructure protection, cross border cooperation and privacy.
  - ⇒ Australia was the primary author of the OECD's Spam Toolkit which provided a multi-pronged strategy to deal with spam. This has improved international cooperation and information sharing on the issue of spam.
  - ⇒ The Working Party was also the vehicle for launching the joint APEC-TEL/OECD work on malware. Current work includes consideration of:
    - ⇒ identity management;
    - ⇒ malware;
    - ⇒ sensor-based environments;
    - ⇒ privacy in light of technology, and globalisation; and
    - ⇒ APEC–OECD work on protection of children online.
  - ⇒ Future work items may include work on generic best practice guidelines for ISPs to provide assistance to their customers on e-security matters. This work could build and potentially expand on work being done on the proposed Australian ISP E-Security Code of Practice.

- **International Multilateral Partnership against Cyber Threats (IMPACT)** is a public-private initiative against cyber-terrorism led by

Malaysia. It is the first global public-private initiative against cyber-terrorism and brings together governments, industry leaders and e-security experts.

- **Forum of Incident Response and Security Teams (FIRST)** conference brings together a variety of computer security incident response teams from government, commercial, and educational organisations. It aims to foster cooperation and coordination in incident prevention to stimulate rapid reaction to incidents, and to promote information sharing among members and the community at large. There is also an associated meeting of national computer emergency response teams (CERTs) known as SECOND that provides a mechanism for cooperation and collaboration to solve many of the issues that national CERTs share in common.[25]

Committee View

5.29 The problem of cyber crime is by its nature an international one and the Committee believes that Australia should maintain a high level of engagement in relevant international fora. However, it is important that resources should not be excessively diverted to these efforts at the expense of developing and implementing concrete measures to assist ordinary Australian consumers and businesses at home.

[25] AGD, *Submission 44*, p.13; DBCDE, *Submission 34*, pp.16-17.

Law Enforcement Coordination

5.30 The following sections focus on the reporting of cyber crime to law enforcement authorities and consumer protection regulators. In particular, it discusses how to improve the reporting and investigation of cyber crime that impacts on end users and small and medium sized businesses. The coordination between Australian law enforcement authorities for investigation of cyber crime and training in the investigation of high tech crime are discussed. Finally, the issue of public-private intelligence sharing across a wider range of cyber crime types is canvassed.

Cyber Crime Reporting and Assistance

5.31 A key issue raised in evidence was the difficulty law enforcement agencies face in addressing complaints about cyber crime from end users. It was said that, in practice, 'online consumers and to a lesser degree businesses, have been left to fend for themselves online'.[26] From a policing point of view, the problem of cyber crime was described as presenting 'unique challenge for governments, particularly law enforcement and crime prevention agencies'.[27] There are several factors that need to be taken into account.

5.32 First, cyber crime is invariably cross jurisdictional, with victims and perpetrators, and sometimes the evidence, all in different jurisdictions. The NT Government said that crimes are 'generally operated by overseas crime groups harvesting bank account details' and transfer funds via 'mules given instructions to send it overseas via Western Union'.[28] This makes close coordination between police forces within Australia and internationally essential.

5.33 Second, as noted above, the nature of cyber crime is highly complex and generally involves a series of interconnected conduct. The combination of activities (spam, malware, adware, spyware, phishing, fake and infected websites, email scams etc) are used together to steal financial credentials and personal identifying information, recruit money mules and ultimately to defraud, trick or steal money on an industrialised scale.[29]

[26] Internet Safety Institute, *Submission 37*, p.9.

[27] Queensland Government, *Submission 67*, p.7.

[28] Northern Territory Government, *Submission 53*, p.1.

[29] AusCERT, *Submission 30*, p.11.

5.34 The combination of these activities frequently engages both civil and criminal legal regimes and involves multiple agencies domestically and internationally.[30] The ACCC, for example, may receive a complaint about fraudulent conduct that also involves the proliferation of malware via spam emails in a phishing attack.[31] In practice, reporting of cyber crime or improper Internet use, if it occurs at all, is distributed across a variety of Commonwealth, State and Territory agencies and private institutions.

5.35 Third, cyber crime activities are generally organised on a large scale but individual incidents are frequently of a small value or have no immediately obvious destructive impact. Consequently, many crimes go undetected providing 'high rewards' for the criminal while attracting 'little attention from police and regulators'.[32] The under-reporting of computer offences where data is compromised through the use of ICT and later used for theft, fraud or other offences is also problematic.[33]

5.36 Additionally, small value crimes often fall below the thresholds applied to trigger an investigation. The CLPC said:

> Investigations and prosecution of many cyber crimes, in particular fraud, is often done on a balance of expenditure and impact. Most Australian states specify a minimum loss threshold, below which an investigation cannot be launched (e.g. $35,000).[34]

5.37 It is possible to commit:

> … credit card fraud of $5 million dollars without attracting investigative attention providing that the amounts stolen per jurisdiction operate below whatever the budget threshold existing in the jurisdiction. Steal $10 from 100 people in NSW another $10 from 100 people in Victoria, another $10 from 1000 people in France, and so forth.[35]

5.38 Measuring the scale of identity crime is also 'hampered by inadequate reporting practices' because a larger proportion of crimes are reported to

[30] For example, Internet Safety Institute, *Submission 37*, p.11; OECD, *Malicious Software (Malware): A Security Threat to* the *Internet Economy*, 2008, pp.22-29; AusCert, *Submission 30*, p.11; Ms Penelope Musgrave, Director, Criminal Law Review, NSW Government, *Transcript of Evidence*, 8 October 2009, p.76.

[31] ACCC, *Submission 46*, p.3.

[32] Internet Safety Institute, *Submission 37*, p.7; see also, Ms Penelope Musgrave, Director Criminal Law Review, NSW Government, *Transcript of Evidence*, 8 October 2009, p.76.

[33] AFP, *Supplementary Submission 25.1*, p.9.

[34] CLPC, *Submission 62.1*, p.9.

[35] CLPC, *Submission 62.1*, p.9.

financial institutions.[36] This, in turn, presents difficulties for police and for policy makers. Dr Russell Smith agreed that there are 'probably too many agencies involved in handling these … issues' and the problem is exacerbated where people report these matters to multiple agencies and institutions:

> They will go to their banks, card issuers, consumer affairs agencies, state and territory police and the Federal Police, and also places like ASIC and the ACCC. So there is a great need for coordination of information.[37]

5.39 Finally, the Committee was also told there is a tendency for Internet economic crimes to be given a 'lower priority and resourcing by police than offline crimes of a similar magnitude'.[38] The ability of police forces, especially at the local level, to accept and respond to the plethora of online criminal activity is limited. The issue is further complicated by the mix of civil and criminal activity involved.

5.40 The result is a lack of capacity in the law enforcement system to aggregate those types of Internet crime that involve 'small impact victimisation distributed across numerous jurisdictions'.[39] This stops law enforcement authorities from 'seeing a true picture' of the volume and scope of the cyber crime problem.[40] In turn, it allows criminal networks to benefit from aggregating the financial reward of dispersed activities, which may have no immediately obvious destructive effect.

5.41 The Committee was told the reason for setting up the first Australian High Tech Crime Centre (AHTCC) in 2003 was to overcome the fragmentation and develop a more coordinated approach. The AHTCC was an attempt by 'Australian law enforcement agencies … to implement a collaborative approach to preventing and investigating technology enabled crime …'[41]

5.42 The purpose of the AHTCC was to coordinate:

> … the information that is coming in so that all of those hundreds of small cases involving small amounts of money would go to one

[36] AGD, *Supplementary Submission 44.1*, p.3.

[37] Dr Russell Smith, AIC, *Transcript of Evidence*, 19 August 2009, p.15.

[38] Internet Safety Institute, *Submission 37*, p.7.

[39] CLPC, *Supplementary Submission 62.1*, p.5.

[40] Mr Alastair MacGibbon, *Cyber security: Threats and responses in the information age*, APSI, December 2009, p.11.

[41] South Australia Police, *Submission 2*, p.3.

> place, and then you would be able to see patterns emerging and put police resources into it.[42]

5.43 It was governed by a national board with high level representation from each of the State and Territory police forces.[43] The website provided information about a range of Internet crime types, and a system of pre-formatted crime reports for malware intrusions and DDOS attacks.[44]

5.44 One of the achievements of the AHTCC was the creation of the Joint Banking and Finance Sector Investigations Team (JBFSIT), to work collaboratively with the finance sector. The JBFSIT, which still exists, takes action against phishing sites targeting Australia financial institutions, mule recruitment sites and malware download sites.

5.45 In November 2007, the Ministerial Council for Police and Emergency Management endorsed the AHTCC becoming a business unit of the AFP.[45] The South Australian Police explained that:

> Most State based law enforcement agencies provided staff and some funding to the AHTCC until it was disbanded in 2007. … Conflicting investigational priorities and an emphasis of addressing Commonwealth priorities to the detriment of State based investigations contributed to the eventual disbandment of the AHTCC in 2007.[46]

High Tech Crime Operations Centre

5.46 The new High Tech Crime Operations Centre (HTCOC) was established in March 2008 as a portfolio within the AFP. The Committee was told that a single portfolio now exists that consolidates all of the AFP 'high-tech investigations arm and high-tech operations support resources'.[47] The role of the HTCOC is to:

- provide a national coordinated approach to combating serious, complex and multi-jurisdictional technology enabled crimes, especially those beyond the capability of single jurisdictions;

[42] Dr Russell Smith, AIC, *Transcript of Evidence,* 19 August 2009, p.15.

[43] Commander Neil Gaughan, AFP, *Transcript of Evidence*, 9 September 2009, p.2.

[44] The AHTCC no longer exists. However, the website remains live and accessible via: <http://www.ahtcc.gov.au/tech_crimes_types/computer_intrusion.htm#report>, viewed 11 January 2009.

[45] Commander Neil Gaughan, AFP, *Transcript of Evidence*, 9 September 2009, p.1.

[46] South Australia Police, *Submission 2*, p.3.

[47] Commander Neil Gaughan, AFP, *Transcript of Evidence*, 9 September 2009, p.2.

- assist in improving the capacity of all jurisdictions to deal with technology enabled crime; and
- support efforts to protect the National Information Infrastructure (NII).

5.47 The AFP stressed the importance of collaboration with the private sector, and with international partners via its network of AFP liaison officers. The JBFSIT continues to operate in Sydney and, in 2008, expanded to Melbourne. An example of this collaboration is with RSA, the Security Division of EMC. RSA submitted that the RSA Anti-Fraud Command Centre has shut down more than 150,000 phishing attacks and reduced the average shutdown time of attacks from 115 hours to five hours. The submitter told the Committee that:

> At the request of Australia's banks for the better good of consumers, RSA is working closely with the High Tech Crime Centre to shut down criminal activity such as phishing attacks.[48]

5.48 The AFP told the Committee that:

> Collaboration with the financial sector is focused on prevention strategies to mitigate the impact of on-line consumers from phishing and malicious software. The analysis of data contained within the portal enables law enforcement to identify those responsible for online fraud activities.[49]

5.49 However, the offenders are 'usually based offshore and collaboration with international partner agencies via the AFP International Network is fundamental to successful investigations and subsequent prosecution outcomes'.[50]

5.50 The effectiveness of these strategies is difficult to measures in terms of prosecutions alone, either in Australia or internationally. In one example, the AFP were successful when 'online covert investigators identified a person attempting to sell a database online belonging to an Australian Domain Registrar':

> The database contained the compromised details of 70,000 Australian online consumers and 12,000 credit cards with an estimated financial exposure of $4.26 million.[51]

[48] RSA, *Submission 28*, p.3.

[49] AFP, *Submission 25*, p.16.

[50] AFP, *Submission 25*, p.16.

[51] AFP, *Clarification regarding High Tech Crime Operations article,* National Media Release, 23 September 2009.

5.51 However, the AFP does not keep statistics on cyber crime reports or prosecutions that involve technology enabled crime. The Committee invited the Commonwealth Director of Public Prosecutions to make a submission to the inquiry, but none was forthcoming. The AGD provided basic statistics that show there has been an average of eight prosecutions annually over the past five years for computer offences under Part 10.7 of the Commonwealth Criminal Code. The majority of the forty-one recorded convictions over the past five years have resulted in fines and bonds, suggesting that these matters fall toward the less serious end of the scale. Five cases have involved imprisonment, and four cases attracted a suspended sentence.[52]

5.52 The Committee also noted CLPC's criticism that Australia's law enforcement strategy puts little emphasis on prosecuting botherders or addressing botnets:

> To date there have been no public prosecutions in Australia of botnet herders. In fact, there is a paucity of prosecutions on the international front as well. Those botnet herders who have been prosecuted tend to come from the lower end of the cybercrime chain, and do not represent botnets run by organised crime groups.[53]

5.53 The CLPC advocated a more proactive approach that targets the dismantling of botnets, which provide the technical infrastructure to launch most of the cyber crime activities. As it was pointed out in Chapter 2, most botnets are self-replicating and self-sustaining and so there is also need for a cleanup process to prevent other criminals from taking over the botnet. The issue of remediation generally is discussed in Chapter 7.

Cyber Crime Reporting

5.54 The HTCOC is not a national focal point for the reporting of cyber crime and, in general, does not take a lead role in coordinating cyber crime investigations. A cyber crime could be reported to the AFP through the local Operations Monitoring Centre or AFP Headquarters. However, the activity must be sufficiently serious or reflect a Commonwealth priority to warrant AFP involvement.[54]

[52] AGD, *Supplementary Submission 44.2*, p.14; note this data does not indicate whether these offences have been prosecuted by Commonwealth or State or Territory authorities.

[53] CLPC, *Submission 62*, p.3.

[54] For example, a large scale DDOS attack on a Commonwealth Government website or hacking and theft from a bank system may warrant an investigation.

5.55 The AFP said that:

> Public reporting is not standardised and public perceptions would be enhanced were a simple uniform system to be introduced. Thus far, public reporting of e-security threats has been facilitated through State and Territory Police, the AFP, and AusCERT. Many of these reports are lodged online via each agency's respective website. However, cases reported are often low level incidents, and not usually critical enough to warrant AFP intervention.[55]

5.56 An incident that is small value and/or impacts only on one individual (or one company) will rank as a low impact crime and is likely to be referred to State or Territory police.[56] Consequently, the AFP does not have a dedicated facility for online reporting of cyber crime or a special hotline reporting number (except in relation to online child sex exploitation) for the general public.[57] The AFP website directs the public (including businesses) to local State or Territory police to report computer offences.[58] However, this is no guarantee that a complaint will be accepted or investigated, as the victim will be usually be asked to report it to the police force of the State where the perpetrator resides or may be referred to another agency, such as the ACCC.[59]

5.57 The Committee was told there is no easy or well known way for someone to report a cyber crime 'whether it is to do with domain names or whatever':[60]

> People know how to report a normal sort of crime. … People who are victims of some sort of cybercrime do not know how or where to report it. If they do front up to their local police station or ring – presumably, it will not be 000 – some authority who they think should be able to take an investigation to the next step, in many cases they have no idea how to handle it either.[61]

[55] AFP, *Submission 25*, p.20.

[56] The assessment of whether an investigation will be undertaken is considered under the framework of the *Case Categorisation and Prioritisation Model* (November 2009).

[57] As noted above, the former AHTCC website did provide for online reporting of a DDOS attack and malware intrusion. The Committee notes that this website is still accessible via a general Internet search but the model is, in fact, defunct.

[58] Commander Neil Gaughan, AFP, *Transcript of Evidence*, 9 September 2009, p.6.

[59] Mr Alastair MacGibbon, Internet Safety Institute, *Transcript of Evidence*, 11 September 2009, p.62.

[60] Mr Paul Brooks, Internet Society of Australia, *Transcript of Evidence*, 9 October 2009, p.6.

[61] Mr Paul Brooks, Internet Society of Australia, *Transcript of Evidence*, 9 October 2009, p.6.

5.58 Mr Paul Brooks, Director, Internet Society of Australia, also observed that cyber crime reporting between the hours of nine to five is inadequate and reporting methods need to be improved.[62] Mr David Ready, a private citizen, expressed his frustration that he was unable to report a phishing site hosted in Australia to the AFP and the Domain Name Registrar one Friday evening in 2006.[63] As Mr Ready pointed out, criminals do not work normal office hours, and, continuation of a fake currency website over the weekend exposed people worldwide to potential victimisation.[64]

5.59 Mr Paul Brooks also stressed that a reporting system must take account of those cases where, for example, an ISP account has been stolen and the user no longer has email. In these cases, complete reliance on an online reporting system would be no improvement.[65]

Recent Innovations in Cyber Crime Reporting

5.60 There have been some innovations with reporting online crime at the State level in recent years. The Queensland Police Fraud and Corporate Crime Group (FCCG) have worked on the problem of 'Nigerian Fraud' through operations Echo Track and Hotel Fortress. An important aspect of this work is the online reporting portal 'for direct reference to the Nigerian Economic Financial Crime Commission and the Ghana Police'.[66] The Committee heard that these operations have so far led to in excess of ten arrests, and one prosecution, in Nigeria.[67]

5.61 The second example, also from Queensland, is the work of the FCCG in conjunction with eBay to establish the 'eBay project'. The eBay project is a 'national web based reporting system' that enables members of the public to report online auction fraud via an 'online reporting function, which includes pre-formatted statements'.[68] Initially the reporting system was only available to eBay users, but has now been extended to all online auction sites. The system collects the essential facts and enables the project to identify potential crimes, making distinctions between civil and criminal matters, and referring offences to the relevant police agency. The

[62] Mr Paul Brooks, Internet Society of Australia, *Transcript of Evidence*, 9 October 2009, p.6.

[63] Mr David Ready*, Submission 6*, p.1.

[64] Mr David Ready*, Submission 6*, p.1.

[65] Mr Paul Brooks, Director, Internet Society of Australia, *Transcript of Evidence*, 9 October 2009, p.7.

[66] Queensland Government, *Submission 67*, p.7.

[67] Detective Superintendent Brian Hay, Queensland Police Service, *Transcript of Evidence*, 17 March 2010, p.3.

[68] Queensland Government, *Submission 67*, p.6.

project also provides police agencies with a single point of aggregated data.[69]

5.62 The Queensland Government implemented the project to relieve the burden on front line local police and to provide a more intelligence based approach to the problem:

> Since the commencement of the eBay project in mid May 2007 there has been a steady acceleration in the number of on-line reports made. As a result the project has served as an invaluable intelligence gathering tool assisting police to identify serial offenders across jurisdictions. In Queensland alone, 788 complaints have been logged to date via this system. It is believed the e-Bay project will allow for more timely investigation and prosecutions by law enforcement agencies thereby limiting the time available for serious offenders to continue committing offences.[70]

Reporting to Consumer Protection Agencies

5.63 There have also been some developments in the field of consumer protection to facilitate cyber crime reporting. The website *ScamWatch* is hosted by the ACCC and functions as a point of access to the work of the *Australasian Consumer Fraud Taskforce*.[71]

5.64 *ScamWatch* is the national platform for disseminating information to the public on how to 'recognise, avoid and report scams'.[72] The public can report a scam to the ACCC via the website and follow links to other State and Territory consumer protection agencies. However, the quality of fraud and scam reporting facilities across these agencies varies. There also appears to be limited capacity to aggregate data received via these reporting mechanisms as there is no comprehensive data collection from these sources.

5.65 To improve information sharing the Auzshare system was created in 2005. Auzshare is a secure online website and database used by the Australian and New Zealand consumer protection authorities to share

[69] Detective Superintendent Brian Hay, Queensland Police Service, *Transcript of Evidence*, 17 March 2010, p.2.

[70] Queensland Government, *Submission 67*, p.6.

[71] The Australasian Consumer Fraud Taskforce is comprised of nineteen government regulatory agencies and departments with responsibility for consumer protection regarding frauds and scams; ACCC, *Submission 46*, p.5.

[72] ACCC, *Submission 46*, p.4.

depersonalised information about complaints, including scams.[73] It enables agencies to issue alerts to each other where there is a cross border issue.

5.66 However, it has also been noted that differing systems and approaches to, for example, categorisation of complaints, reduces the effectiveness of Auzshare.[74] The Productivity Commission's review of the Australian consumer protection framework has also 'highlighted the benefits of a linked complaints information system, and the need for comprehensive and consistent data provisions'.[75]

eConsumer.gov

5.67 In addition, the eConsumer.gov site provides a complaint portal where consumers from anywhere in the world can report a scam involving a foreign company that appears to be located in a member country.[76] The reporting facility is an initiative of the International Consumer Protection and Enforcement Network (ICPEN). The information contained in the 'complaint is entered into Consumer Sentinel, a consumer complaint database maintained by the US Federal Trade Commission'.[77]

5.68 The data is accessible to certified government law enforcement and regulatory agencies in ICPEN-member countries and is used to 'investigate suspect companies and individuals, uncover new scams, and spot trends in fraud'.[78] Information submitted through the online complaint form may be used to aggregate the data to analyse trends and statistics that may be released to the public.

5.69 These initiatives in both in the traditional criminal law and consumer protection areas demonstrate the potential for systems to improve public reporting on a range of cyber crime activity, and the opportunity to use that data to analyse large scale activity, support investigations, analyse trends and help measure the scale of the problem.

[73] ACCC, *Supplementary Submission 46.1*, p.2.

[74] Mr Peter Kell, Deputy Chair, ACCC, ACFT Consumer Fraud Research Forum, *Consumer Complaints about Scams: Managing and Sharing Information,* October 2009.

[75] Mr Peter Kell, Deputy Chair, ACCC, ACFT Consumer Fraud Research Forum, *Consumer Complaints about Scams: Managing and Sharing Information*, October 2009.

[76] ACCC, *Submission 46*, p.7.

[77] ICPEN, viewed 18 January 2009, <http://www.econsumer.gov/english/report/overview.shtm>.

[78] ICPEN, viewed 18 January 2009, <http://www.econsumer.gov/english/report/overview.shtm>.

A New National Approach to Cyber Crime Reporting

5.70 Several submitters proposed the creation of a national body to establish a more coherent response to victims and improve strategic capacity to detect and pursue online crime. Dr Russell Smith told the Committee there are now central reporting agencies in the UK, the US and Canada and:

> If they are adequately funded, I think they can make some inroads into solving some of the problems.[79]

5.71 In the US, the Internet Crime Complaints Centre provides an online reporting mechanism for the public to make complaints of cyber crime, especially online fraud, and functions as a clearing house on cyber crime.[80] The Centre is managed by the FBI and works closely with other bodies, such as the US Cyber Forensics and Training Alliance (NCFTA). The Federal Trade Commission and other agencies also take reports of various cyber crime types.

5.72 In the UK the Police Centre e-Crime Unit is located within the Serious and Organised Crime Agency (SOCA), with a remit to investigate serious e-crime.[81] However, it does not take reports from individual members of the public and the decentralised policing structure has made analysis at the national level difficult.[82] Under a recently adopted *ACPO e-Crime Strategy* the National Fraud Reporting Centre was designated as the national reporting centre for cyber crime.[83] As part of the *National Fraud Strategy*, investigators can now take cases that individually may not have been investigated but together represent significant loss.[84]

5.73 The NSW Government argued that consumers would benefit greatly from centralised cyber crime reporting:

> At present, agencies such as ACMA and others provide an avenue for reporting some cyber crimes (eg spam), but the broad range of

[79] Dr Russell Smith, AIC, *Transcript of Evidence,* 19 August 2009, p.15.

[80] Queensland Government, *Submission 67*, p.7.

[81] The SOCA e-Crime Unit is separate from the Child Exploitation and Online Protection Centre. Cases that fall within the PCeU Case Acceptance Criteria include: significant intrusions into government, commercial or academic networks; denial of service attacks, and other criminal use of Botnets; significant data breaches; significant false identity websites; mass victimisation e-crimes, such as large scale phishing, and electronic attacks on the Critical National Infrastructure, *ACPO e-Crime Strategy*, 2009, p.8.

[82] *ACPO e-Crime Strategy*, 2009, p.2.

[83] The City of London Police, which has been designated the National Lead Police Force for Fraud, hosts the facility.

[84] Jeremy Kirk, IDG New Service, UK Police to Track E-Crime, *Fraud Down to the Last Pence*, 25 March, 2009.

> cyber-scams that now exist suggest that the community may be better served by providing a central point to refer suspected cyber-scams, rather than the segmented and ad-hoc arrangements currently in place.[85]

5.74 Detective Inspector William van der Graff commented that a lot of resources are devoted to the problem of online scams but there are few prosecutions:

> I would like to see a national body that looks at this data and launches prosecutions of people internationally. I should say it is not necessarily easy. We are doing one at the moment and the people we are trying to track are very good. We may not meet with success in this case, but until we attempt it we do not know.[86]

5.75 The Queensland Government suggested a Centre, like the FBI Internet Crime Centre, complemented by an E Crime Mangers Group. The E Crime Mangers Group would have representation from each Australian policing agency.[87] It would promote national coordination, facilitate inter-jurisdictional operations, establish national standards and facilitate information sharing.[88]

5.76 AusCert and the Internet Safety Institute argued for a more integrated and consumer focused centre that can provide an Internet wide perspective to the problem.[89] To achieve a more effective response to the range of cyber crime activity will require a higher level of cooperation between civil and law enforcement agencies.[90]

5.77 In a recent paper for Australian Strategic Policy Institute, Mr Alastair MacGibbon, Director, Internet Safety Institute said that:

> Australia needs an internet crime reporting and analysis centre for homes and businesses. The relevant federal law enforcement and consumer protection agencies are not constituted, staffed, or able

[85] NSW Government, *Submission 49*, p.6.

[86] Detective Inspector William van der Graff, NSW Police Force, *Transcript of Evidence*, 8 October 2009, p.77.

[87] Queensland Government, *Submission 67*, p.7.

[88] Queensland Government, *Submission 67*, p.7; By contrast, the UK Police Service has already established standards for professional practice within e-crime, such as the *ACPO Good Practice Guide for Computer Based Evidence* and the *ACPO Managers Guide to e-Crime*; *ACPO e-Crime Strategy*, 2009, p.18.

[89] Mr Graham Ingram, Director, AusCERT, *Transcript of Evidence,* 11 September 2009, p.5; Mr Alastair MacGibbon, Director, Internet Safety Institute, *Transcript of Evidence*, 11 September 2009, p.62.

[90] AusCERT, *Submission 30,* p.15; Internet Safety Institute, *Submission 37*, pp.3 and 10.

> to deal with the often small and seemingly inconsequential incidents of fraud, spam, scams, data loss, inappropriate content, or sometimes IT security incidents. We need an Internet 'shopfront' approach. A place for people to report matters, and to seek advice: a single consumer orientated destination, scaled for the Internet, which takes a national whole of government approach.[91]

5.78 In evidence to the Committee, Mr Alastair MacGibbon explained the purpose of centralised reporting would be to provide a one stop shop for the public and small businesses who believe they are a victim of cyber crime. It would operate on a 24 hour 7 day a week basis and be a combined public and private project. The aim would be to: provide a simple reporting mechanism for ordinary consumers: improve data collection, and intelligence analysis and sharing across police forces and other agencies; support targeted prosecutions; better identification of cyber crime trends; and provide education on e-security risks.[92]

5.79 The reporting system would provide for standardised first instance reporting and data collection on a range of cyber crime types. Police services would need to learn about large scale reporting, because these crime types involve large numbers of incidents that occur in a fragmented way.[93]

> An internet crime reporting and analysis centre would be most successful as a public-private partnership which could allow real-time information flow between the government's CERT Australia and the Cyber Security Operations Centre, giving Australia a more holistic view of Australia's internet health, and improving our ability to respond to threats and rebound.[94]

5.80 The IT company, McAfee, expressed strong support for working with other partners to establish a centralised online reporting mechanism for the general public in Australia. In the US, McAfee has already launched the *Cybercrime Response Unit* (CRU), an online portal for consumers and small and medium sized businesses. The CRU provides education about

[91] Mr Alastair MacGibbon, *Cyber security: Threats and responses in the information age*, Australian Strategic Policy Institute, December 2009, p.11.

[92] Mr Alastair MacGibbon, Director, Internet Safety Institute, *Transcript of Evidence*, 11 September 2009, p.62.

[93] Mr Alastair MacGibbon, Director, Internet Safety Institute, *Transcript of Evidence*, 11 September 2009, p.62.

[94] Mr Alastair MacGibbon, *Cyber security: Threats and responses in the information age*, Australian Strategic Policy Institute, December 2009, p.11.

online behaviours that lead to higher risks of cyber crime, and provides links to resources to report online crimes.[95]

5.81 The CRU includes free access to a 'non-intrusive' scanner that checks the PC to identify possible weaknesses in the owner's computer and risky online behaviour. The scan produces a report with recommendations on what the user can to do protect themselves from online threats. The issue of remediation of infected machines is discussed in Chapter 7.

5.82 McAfee funds all aspects of the portal, including CRU staff to answer victims' questions and clarify where to report the crime.[96] McAfee also told the Committee that it has developed close working relationships with US, European and British enforcement authorities. It shares intelligence on latest threat advice, and provides specific case support.[97]

5.83 On request by the Committee, McAfee expanded on the detail for a similar but more advanced model for Australia.[98] The company said it is willing to fund an Australian e-security portal that would also provide a 'central gateway' notifying appropriate agencies of incidents of cyber crime and:[99]

> … is willing to provide additional resources to ensure that law enforcement, financial service providers, and telecom service providers have the intelligence from this portal that they need to use the information effectively.[100]

5.84 Central reporting would enable more effective use of resources and quicker response times through the:

> … cross analysis of victim reports across Australian jurisdictions, combined with our Global Threat Intelligence or reputation-based scoring of cyber crimes and their websites globally… [101]

5.85 One of the benefits of central reporting is that it:

> … could greatly enhance law enforcement's ability to respond to only the immediate crimes and not spend as much time fielding general questions and following information that is not necessarily

[95] McAfee, *Submission 10*, pp.11-12.

[96] McAfee, *Supplementary Submission 10.1*, pp.2-4.

[97] McAfee, *Supplementary Submission 10.1*, p.3.

[98] McAfee, *Supplementary Submission 10.1,* pp.1-3.

[99] McAfee, *Supplementary Submission 10.1*, p.3.

[100] McAfee, *Supplementary Submission 10.1*, p.2.

[101] McAfee, *Supplementary Submission 10.1*, p.3.

> in and of itself, an online crime or one in which no usable information is available.[102]

5.86 The aim would be to provide a technical solution to e-crime reporting but, the company stressed, collaboration between Federal, State and Territory police forces would remain critical to ensure suitable action is taken in response to incident reports.[103]

5.87 Detective Superintendent Brian Hay, Queensland Police Service, suggested that such a reporting centre should sit with an agency outside of the law enforcement sphere:

> A federal agency would be an appropriate body. If you look at the UK model, it has a non-law enforcement agency as the lead agency. The United Kingdom's National Fraud Authority is the lead agency for the reporting portal, but it is not a law enforcement agency. So I would be looking at a federal agency that is not the police, because a lot of the issues that will come forward are very much consumer based issues.[104]

5.88 McAfee also suggested that monetary thresholds should be removed.[105] By way of example, McAfee referred to the US *Identity Theft Enforcement and Restitution Act*, passed in September 2008 to eliminate the previous threshold of $5,000.[106] Instead of filtering out complaints via a financial threshold that inhibit investigations, the model recognises the dispersed nature and impact of computer based identity crimes. The penalty provisions are also triggered by an estimate of the aggregated losses resulting from a crime that victimises more than one person.[107]

5.89 The Committee has no evidence that any Australian jurisdiction has legislated money thresholds. However, it was suggested that an explicit mechanism to ensure that cyber crime incidents, including small value crimes, can be multiplied across police forces may be necessary. The CLPC suggested that a Memorandum of Understanding or, if necessary, a legal

[102] McAfee, *Supplementary Submission 10.1*, p.2.

[103] McAfee, *Supplementary Submission 10.1*, p.3

[104] Detective Superintendent Brian Hay, Queensland Police Service, *Transcript of Evidence*, 17 March 2010, p.9.

[105] McAfee, *Submission 10*, p.7.

[106] McAfee, *Submission 10*, p.7.

[107] Section 1030 Title 18 of the *United States Code*; Roy Jordan, *Client Memorandum*, Department of Parliamentary Services, 12 January 2010; the penalty for computer offences resulting in an aggregated loss to one or more person of at least $5,000 (over a twelve month period) attracts a fine of up to 5 years imprisonment (or both).

provision, should be adopted between Australian police forces (and internationally) to facilitate the aggregation of shared intelligence.[108]

Committee View

5.90 The evidence highlighted two interrelated issues that arise from Australia's current approach to the incidence of cyber crime and cyber crime reporting.

5.91 First, it is difficult for end users to know where to report an e-security incident (whether malware intrusions or identity fraud) and probably a degree of uncertainty over what redress is available. Under-reporting means that it is difficult to measure the size of the problem and, if reporting does occur, an incident could be reported to multiple agencies and private institutions.

5.92 The second and related issue is the lack of a nationally scaled institutionalised capacity to systematically collect and aggregate the intelligence data. There is no standardised method for receiving reports of e-crime from the general public or from companies that want to report. Nor is there any clear mechanism for sharing information on cyber crime reports between police forces, or between criminal and civil agencies such as the ACCC. This means lost opportunities for strategic intelligence analysis and detection of organised crime and support for prosecution in Australia or overseas.

5.93 A central reporting portal would enable reporting across the range of cyber crime types (malware, spam, phishing, scams, identity theft and fraud etc). Data collection and analysis would strengthen the detection of organised crime and support law enforcement efforts across jurisdictions. It would also provide existing agencies such as CERT Australia and the Cyber Security Operations Centre a more complete view of criminal activity on the Internet.

5.94 Where a consumer has suffered a malware intrusion, free access to scanning software and, where necessary, specialised IT assistance to remediate infected machines would help prevent re-victimisation. Remediation is discussed in Chapter 7. Information about cyber crime threats and e-security alerts, such as the Stay Smart Online alert service, and information about preventative e-security measures could also be integrated into the one body.

[108] CLPC, *Supplementary Submission 62.1*, p.9.

5.95 To maximise its effectiveness the body should be staffed by suitably qualified analysts and investigators, who could be dedicated or seconded from the various agencies, including the research staff from the Australian Institute of Criminology. Specialist banking and fraud investigators funded by the private sector will be integral and, in the Committee's view, should be funded by the private sector.

Recommendation 4

That the Australian Government, in consultation with the State and Territory governments and key IT, banking and other industry and consumer stakeholders, develop a national online cyber crime reporting facility geared toward consumers and small and medium sized businesses.

This model should include the following features:

- **a single portal for standardised online receipt of cyber crime reports across a wide range of cyber crime types (e.g. malware, spam, phishing, scams, identity theft and fraud);**
- **a 24/7 reporting and helpline;**
- **no financial minimum to be applied to cyber crime reports;**
- **systematic data collection that allows data to be aggregated;**
- **referral to appropriate authorities and cooperation the on disruption and cyber crime and targeted prosecutions;**
- **free access to scanning software to detect malware;**
- **public information about cyber crime types and preventative measures to increase online personal security;**
- **e-security alerts tailored to the needs of ordinary consumers and small and medium sized businesses; and**
- **analysis of cyber crime methodologies and trends or cooperation with another body to perform that analysis.**

Criminal Law Enforcement Coordination

5.96 The NSW Government contended that the HTCOC has a role to 'provide a national approach to combating cyber-crime especially where the abilities of a particular jurisdiction are limited.'[109] However, the Tasmanian Government submitted that 'since the closure of the AHTCC there has not been significant cross-jurisdictional coordination in relation to e-security risks'.[110]

5.97 The NT Government also said that:

> It was hoped when the AHTCC was established in 2003 that it would provide a liaison with international police and help coordinate offences from the Australian end and refer them overseas. From an NT Police perspective the AHTCC appears to be focused primarily on internet banking fraud and is not in a position to offer substantial assistance in the other areas… [111]

5.98 The AFP considered that the former AHTCC was an 'effective model for undertaking investigation and sharing information and expertise' because it was a national body and provided a consistent approach.[112] While it aims to build on those relationships, Commander Gaughan agreed that coordination with State and Territory police is 'where the difficulty currently lies'.[113]

5.99 The Australian Banking Association (ABA) argued that at the national level, the difficulties encountered in fighting cyber crime are not legal jurisdictional issues but 'differing priorities between agencies on prevention, detection and prosecution'.[114] There is a 'need for more coordination and cooperation between agencies in sharing vital information and intelligence risks (prevention)'.[115] At the present time

[109] NSW Government, *Submission 49*, p.4.

[110] Tasmanian Government, *Submission 51*, p.4.

[111] NT Government, *Submission 53*, p.2.

[112] AFP, *Submission 25*, p.15.

[113] Commander Neil Gaughan, AFP, *Transcript of Evidence*, 9 September 2009, pp.2-3.

[114] ABA, *Submission 7*, p.6.

[115] ABA, *Submission 7*, p.7.

there is no national centralised mechanism for coordinating these activities.[116]

5.100 Similarly, the South Australia Police said that there is no 'coordinated medium for information to be exchanged about crime trends and methods'.[117] The re-establishment of the E-Crime Investigation Managers Committee under the auspices of Australian New Zealand Police Advisory Agency (ANZPAA) may improve information exchange. However, there was no suggestion that this alone would be sufficient.[118]

5.101 It was noted that the capacity of consumer protection and law enforcement agencies to respond varies across the jurisdictions. The highly technical nature of these crime types requires specialist skills and equipment.[119] Most State and Territory police forces have specialist investigators and some capacity for forensic analysis. The NSW Police has the NSW Police Fraud Squad Computer Crime Team and South Australia Police has a small Electronic Crime Section comprised of a manager, five investigators and four electronic evidence specialists.[120] But smaller jurisdictions, such as Tasmania, have less capacity to address the problem.[121]

5.102 The Tasmanian Government argued that cyber crime can only be properly addressed at the national level:

> Many e-security issues affect consumers across Australia and internationally, and consequently it is not practical for State agencies to address them individually. Further, responses by individual states risks significant duplication of resources, which can be ill-afforded by small jurisdictions. This is especially the case with regard to highly technical problems such as those posed by the increasing criminal use of malware.[122]

5.103 The lack of national coordination means that cooperation between police forces operates on a case by case basis with police services across Australia 'providing assistance or referrals to one another'.[123]

[116] ABA, *Submission 7*, p.6.

[117] South Australian Police, *Submission 10,* p.4.

[118] South Australian Police, *Submission 10,* p.4.

[119] NSW Government, *Submission 49*, p.4.

[120] South Australia Police, *Submission 2*, p.1.

[121] Tasmanian Government, *Submission 51*, pp.1-5.

[122] Tasmanian Government, *Submission 51,* p.5.

[123] Tasmanian Government, *Submission 51*, p.4.

5.104 'Pending the development of a more formal coordination mechanism', Tasmanian investigators have joined the AUSPOL email list hosted by AusCERT.[124] AUSPOL enables e-crime investigators to share information by posting 'queries and information to their colleagues across the country.'[125]

Training and development

5.105 There was also a call from some police forces for a more coordinated approach to training and development, which the Committee was told is expensive and only happens on an ad hoc basis. South Australia Police argued that there is a lack of 'consistency in the frequency and level of training provided to law enforcement detectives involved in investigating technology enabled crime'.[126] This area of crime requires regular upgrading of skills as new technologies means that 'new investigative techniques are required'.[127] It was suggested that minimum standards should be set and processes established to ensure the capacity of the police to respond to technology enabled crime is maintained.[128]

5.106 The NSW Government proposed the creation of a National Cyber Crime Training Institute that could be the centre of training and skills development for police working in this field.[129] Detective Inspector William van der Graff, Coordinator, Computer Crime Team, Fraud Squad, NSW Police Force, argued that such a body would be an effective way of ensuring over the longer term that sufficient numbers of police officers are adequately skilled in this area.[130] Although a National Cyber Crime Training Institute would primarily serve the needs of law enforcement agencies, he suggested that it could potentially also provide training for other arms of government.[131]

[124] Tasmanian Government, *Submission 51*, p.4.

[125] Tasmanian Government, *Submission 51*, p.4.

[126] South Australia Police, *Submission 2*, p.3.

[127] South Australia Police, *Submission 2*, p.3.

[128] South Australia Police, *Submission 2*, p.3.

[129] Detective Inspector William van der Graff, NSW Police Force, *Transcript of Evidence*, 8 October 2009, p.77.

[130] Detective Inspector William van der Graff, NSW Police Force, *Transcript of Evidence*, 8 October 2009, p.77.

[131] Detective Inspector William van der Graff, NSW Police Force, *Transcript of Evidence*, 8 October 2009, p.77.

5.107 AGD informed the Committee that the AFP offers electronic crime based training courses to other Commonwealth, State and Territory law enforcement agencies. The includes the AFP's:

- Internet Policing Program which provides training in the tactical use of the Internet including online conversations with suspects and advanced internet search techniques;
- Child Protection Operations workshop which provides training for investigating online child sex offences and child sex tourism internationally with a focus on the nexus between international law enforcement, the AFP and State and Territory police; and
- Management of Serious Crime course, a multi-agency, multi-jurisdictional program provided to a range of senior law enforcement practitioners across the Commonwealth and the States and Territories that includes a focus on cyber crime investigations.[132]

5.108 The AGD also told the Committee that the AFP is establishing a Technology Enabled Crime Centre of Excellence within its High Tech Crime Operations portfolio:

> This Centre brings together technical, legal and other subject matter experts to provide the AFP and its partner agencies with a single point of contact on issues of technology enabled crime. The Centre is being formed in recognition of the increasing complexity of technology enabled crime and the need to deliver contemporary, specialist advice to investigators working on these matters.[133]

5.109 In June 2009, the AFP hosted the Australian High Tech Crime Conference with the University of Technology, Sydney and the Australian Institute of Criminology. Such conferences were said to be useful to develop and maintain links between law enforcement, the judiciary, the legal profession, academia, industry experts and government officials. AGD said:

> The conference was successful in sharing information, ensuring a dialogue on key challenges, addressing investigative techniques and discussing legal and legislative issues relating to technology based crimes. The AFP will continue to host this conference annually.[134]

[132] AGD, *Supplementary Submission 44.2*, p.11.

[133] AGD, *Supplementary Submission 44.2*, p.11.

[134] AGD, *Supplementary Submission 44.2*, p.11.

Committee View

5.110 The measures outlined by AGD will all contribute to building better law enforcement capacity and provide opportunities to share information and skills. However, the Committee believes that the proposal for an E Crime Managers Group and a National Cyber Crime Training Institute have considerable merit, and would go a long way toward ensuring a more effective harnessing of police resources.

5.111 The responsibility for developing and maintaining these structures should be shared across all Australian governments, to ensure that such measures are responsive to the needs of all jurisdictions.

Recommendation 5

That the Federal, State and Territory police forces establish an E Crime Managers Group to facilitate the sharing of information and cross jurisdiction cooperation.

Recommendation 6

That the Australian Government, in consultation with the State and Territory governments, industry and consumer organisations, develop a national law enforcement training facility for the investigation of cyber crime.

Public-Private Cyber Crime Intelligence Sharing

5.112 Many witnesses emphasised the importance of the government and private sector 'working together to improve computer security', both in relation to critical infrastructure and the wider area of cyber crime that impacts on Australian society more broadly.[135] The evidence indicated a need for intelligence sharing on a wider range of cyber crime types and this information to be both:

- in real time operational intelligence; and

[135] See for example: Microsoft, *Submission 35*, p.11; Australian Information Industry Association, *Submission 22*, p.12; AGD, *Submission 44*, p.11.

- longer term analysis and information sharing within and between industries; and
- be based on pre-sanctioned trusted information sharing networks.

5.113 As noted above, the Australia Government has recently established the DSD Cyber Security Operations Centre and, in collaboration with AusCERT, moved to bring computer emergency response team functions together under CERT Australia. The primary mechanism for public-private sharing of sensitive security related information remains the pre-existing Trusted Information Sharing Network for Critical Infrastructure Protection (TISN).[136]

5.114 Under the umbrella of the TISN, CERT Australia will now operate the three sectoral exchanges to share technical information in the:

- banking sector;
- communications sectors; and
- owners and operators of control systems in power and water utilities.[137]

5.115 Witnesses made several points about the nature of the public-private collaboration. The first issue was the scope of the existing TISN, which is focused on national security and critical infrastructure. For example, Telstra said:

> Within the current national critical infrastructure framework of the existing Trusted Information Sharing Network (TISN) … focus is specifically on the national security context of cyber crime (i.e. e-security). The existence of this framework may provide an opportunity to extend the TISN focus into cyber crime and its impact on Australian society more broadly.[138]

5.116 The ABA also expressed concern that the existing TISN does not cover all the types of cyber crime intelligence that interest the banking sector:

> Strict boundaries between national security, critical infrastructure protection, financial crimes and other non-financial crimes may no longer be appropriate as the mechanisms used by cyber criminals are common to all.[139]

5.117 The ABA explained that they want to see a more integrated approach:

[136] AGD, *Submission 44*, p.10.

[137] AGD, *Submission 44*, p.11.

[138] Telstra, *Submission 43*, p.3.

[139] Mr Tony Burke, ABA, *Transcript of Evidence,* 8 October 2009, p.51.

> In terms of the traditional intelligence cycle this probably means the centralisation of the planning and direction, analysis and production functions with sharing of the collection, processing and dissemination functions.[140]

5.118 The ABA, advocated a 'more formal arrangement for sharing intelligence with its Members' and said that:

> No governing body currently exists to allow strategic threats to be continually assessed between the public and private sectors (other than in the area of Critical Infrastructure) in this area.[141]

5.119 Given the interdependency of the public and private sectors, the ABA said this situation 'places Australian institutions in both the public and private sector at a disadvantage when it comes to protecting Australian internet users'.[142]

5.120 Mr Richard Johnson, Chief Information Security Officer, Westpac Banking Corporation, told the Committee that while relationships have been developed with 'segments of the banking industry, the AFP and some other government bodies, these relationships are effectively point-to-point, personal based relationships….':

> The large number of working groups, advisory groups, government agencies, departments and law enforcement bodies may be better served by a single point of coordination on cyber crime issues and information exchange.[143]

5.121 RSA also submitted that private industry associations and their security solution providing members cannot 'gain the upper hand on their own' and called for a more centralised and coordinated leadership from the Australian Government.[144]

5.122 In addition to the scope of the TISN, some witnesses commented on the nature of the trust relationship and indicated some concern about the timeliness of information. Mr Johnson, Westpac, said the key to trusted relationships is the 'free and open bidirectional sharing of information and intelligence'.[145] The witness told the Committee there is a lack of

[140] Mr Tony Burke, ABA, *Transcript of Evidence,* 8 October 2009, p.51.

[141] ABA, *Submission 7,* p.13.

[142] ABA, *Submission 7,* p.14.

[143] Mr Richard Johnson, Westpac Banking Corp, *Transcript of Evidence*, 8 October 2009, p.52.

[144] RSA, *Submission 28*, p.3.

[145] Mr Richard Johnson, Westpac Banking Corp, *Transcript of Evidence*, 8 October 2009, p.52.

formalised and pre-sanctioned trust relationships between government and industry and this has:

> … left both groups effectively unsure of exactly what can be shared. Information that is shared is therefore redacted to such a point that it borders on being meaningless. In other words, we do not know what we do not know.[146]

5.123 Importantly, the apparent lack of pre-sanctioned relationships was said to affect the timeliness of sharing real time operational intelligence. Mr Johnson, Westpac, explained that:

> Timeliness of this information is critical to be effective. Cybercrime threats, by their very nature, are given to evolve rapidly. Current information-sharing arrangements are dependent on multiple levels of clearance and release approval, severely limiting the usefulness of information that can be shared. A true national, trusted intelligence-sharing network is required, with preclearance of participants and of the information types which can be shared. This needs to operate in real time to match the nature of the threat. By sharing information and pooling data, analysis of the entire dataset can be performed and each participant will gain a holistic view of the common threat which today we can each only see from our own point of view.[147]

5.124 Symantec, a global IT security vendor, also provided comment on the TISN. In particular, Symantec said that trust, time and resources are the key to public-private cooperation and it was important for the relationship to be one of exchange. For example, offering participants exclusive cyber threat intelligence information that cannot be obtained elsewhere. Symantec also observed that private sector members need assurance on key issues such as:

- the role and intention of authorities requesting information;
- whether there is exposure to regulatory enforcement action;
- protection of commercially sensitive information; and
- the protection of privacy of consumers.[148]

5.125 The witness proposed that Australia consider enacting legislation to assure private sector participants that confidential, proprietary, and

[146] Mr Richard Johnson, Westpac Banking Corp, *Transcript of Evidence*, 8 October 2009, p.53.

[147] Mr Richard Johnson, Westpac Banking Corp, *Transcript of Evidence*, 8 October 2009, p.53.

[148] Symantec, *Supplementary Submission 32.1*, p.8.

business-sensitive information is only used for the purpose for which is it shared. In particular, that the information is protected from public disclosure, regulatory action, and there are uniform procedures for receipt, care and storage of information. Symantec advised that, in the context of critical infrastructure, the US introduced the *Critical Infrastructure Information Act 2002* to improve information sharing. An alternative would be formalised and enforceable data sharing and non-disclosure agreements, however, it was noted that these agreements are likely to still entail the possibility of regulatory and legal action.[149]

5.126 Further evidence from AGD opposed any specific legislation and argued that existing arrangements are adequate, and include legal remedies for breach of confidentiality. Private sector organisations sign a *Deed of Confidentiality*, which set out their obligations:

> This ensures that information is properly managed and reasonably protected from unauthorised disclosure or use. Information that is provided to Government within the TISN is used for legitimate TISN purposes only. This information is not disclosed to other regulatory agencies, unless required by law. In such cases, the owners of the information would be given prompt notice and reasonable details of the circumstances involved should they wish to respond.[150]

5.127 Additionally, public sector officials sign a *Government Representative Confidentiality Acknowledgement,* which acknowledge their statutory and other legal and policy obligations for information handling.[151]

5.128 Symantec also suggested a standardised structure for the exchange of information that describes, categorise, prioritise information and have established channels for the escalation of security incidents. Two examples of messaging standards for information sharing purposes were the EU Messaging Standard for Sharing Security Information (MS3i), and the US National Information Exchange Model (NIEM).[152]

5.129 Symantec also proposed that appropriate house rules be established on participation in sector meetings. This was intended to ensure minimum levels of seniority and the involvement of decision makers to generate

[149] Symantec, *Supplementary Submission 32.1*, p.9.

[150] AGD, *Supplementary Submission 44.2*, pp.1-2.

[151] These include section 70 of the *Crimes Act 1914* (Cth) which deals with disclosure of information by Commonwealth officers, the *Australian Public Service Code of Conduct* set out in the *Public Service Act 1999* (Cth) and the Australian Government's Protective Security Manual.

[152] Symantec, *Supplementary Submission 32.1*, p.9.

trust. The Warning, Advice and Reporting Point (WARP) in the UK was given as an example.[153]

5.130 The Committee also heard from Ms Alana Maurushat, Deputy Director, CLPC who advocated the creation of a body similar to the US National Cyber Forensics and Training Alliance (NCFTA).[154] The NCFTA is not a law enforcement agency. It operates as an intelligence hub receiving intelligence from companies and organisations that are victims of cyber crime (DDOS attacks, security breaches, fraud).[155]

5.131 The NCFTA can work across industry sectors to aggregate intelligence, assisting organisations to mitigate attacks, preserve digital evidence, and work with law enforcement to support prosecutions.[156] In her view, the creation of an 'intelligence hub' is 'really important for Australia and what is grossly lacking'.[157]

5.132 Dr Paul Brooks, Director, Internet Society of Australia made the distinction between real time operational information and the longer term analysis:

> When somebody notices that their equipment, their ISP or their home PC has been hacked, it requires different tools, a different level of investigative ability and a different organisations structure for them to be able to pick up the phone and get on a hotline to somebody who can within minutes identify what is going on a try and tack that back in real time to where it is coming from so you can actually catch the guys that are doing it.[158]

5.133 From an industry perspective, Mr Richard Johnson, Westpac Banking Corporation, submitted that in the US the Information Sharing and Analysis Centres (ISACs) are industry based centres that provide a real time information sharing network. This is operational intelligence on threats that are underway:

> That is the kind of operation level intelligence we … need to develop which then, for a strategic analysis purpose, could be fed into the research alliances.[159]

[153] Symantec, *Supplementary Submission 32.1*, p.9.

[154] CLPC, *Submission 62*, p.11.

[155] Ms Alana Maurushat, CLPC, *Transcript of Evidence*, 8 October, 2009, p.33.

[156] CLPC, *Submission* 62, p.11.

[157] Ms Alana Maurushat, CLPC, *Transcript of Evidence*, 8 October, 2009, pp.32-33.

[158] Dr Paul Brooks, Internet Society of Australia, *Transcript of Evidence,* 9 October 2009, p.13.

[159] Mr Richard Johnson, Westpac Banking Corp, *Transcript of Evidence*, 8 October 2009, pp.54-55.

5.134 Mr Johnson also advised the Committee that the company has been involved in creating the Internet Commerce Security Laboratory, a joint research alliance with the Victorian Government, the University of Ballart and IBM, with support of the AFP. The Internet Commerce Security Laboratory is a research facility that performs data mining, data analysis and correlation to provide better leads, intelligence and information to support arrests.[160]

Committee View

5.135 The Committee considers that public-private cyber crime intelligence coordination is vital to achieve a more resilient Internet and ICT environment and ensure confidence in the digital economy. This view is also reflected in the Australian Government's recent *Cyber Security Strategy.*

5.136 Under the *Cyber Security Strategy*, the new DSD Cyber Security Operations Centre is geared to detect and respond to aggressive cyber attacks on the 'National Information Infrastructure'.[161] It supports non-government critical infrastructure through ASIO, AFP and AGD. CERT Australia obtains cyber threat intelligence and, through the three sector exchanges, shares technical information with the banking, utilities and communications sectors. This is in the context of national security and critical infrastructure protection.

5.137 However, the evidence to the Committee was that there is also a need to either:

- widen the remit of CERT Australia and TISN to encompass a broader range of cyber time types; or, alternatively;
- create separate and additional capacity through a joint public-private organisation to obtain, analyse and share technical real time actionable information.

5.138 The evidence indicates that Government leadership with significant private sector participation is needed to address the current lack of coordinated response to a wider range of cyber crime types that impact Australian society more generally.

[160] Mr Richard Johnson, Westpac Banking Corp, *Transcript of Evidence*, 8 October 2009, pp.54-55.

[161] The national information infrastructure is made up of those key communications and information technology systems that support critical industries and government services, such as the telecommunications, transport, distribution, energy, utilities, banking and finance industries and defence and emergency services.

5.139 A Government led initiative to develop a more coordinated approach to accessing and sharing real time operational data was a high priority for several witnesses. There was also consistent advocacy for some form of 'intelligence hub(s)' for analysis of methodologies and trends, and, where possible, support targeted prosecutions in Australia and internationally.

5.140 At first glance it might appear logical to integrate these functions into the same organisation. However, the evidence indicates that these functions are distinct and require different types of organisations albeit with close links. The former must be genuinely responsive and operate through a network of pre-sanctioned relationships in a clearly visible and accepted trust environment. This may require special legislation to provide the visibility necessary to build trust between government and the private sector and between competitors.

5.141 The latter is focused on the deeper and longer term analysis of methodologies and trends that can support industry preparedness. This could include cross industry intelligence sharing, private sector education on the preservation of digital evidence, and, where possible, support to targeted law enforcement action in Australia and overseas.

5.142 The Committee is aware that other countries face the same challenges and have useful experience to draw on. In the US, for example, a network of public-private Information Sharing and Analysis Centres provide real time operations intelligence for critical infrastructure. This approach might provide an effective model for intelligence sharing on the wider cyber crime types in Australia. The NCFTA is also a model for cross industry intelligence gathering and analysis. However, some steps have been taken in that direction with the creation of the Internet Commerce Security Laboratory.

Recommendation 7

That the Australian Government consult with major IT security vendors, academia and key industry stakeholders to develop:

- **options for establishing a coordinated public-private capacity to provide real time operational information on a wider range of cyber crime types that impact on Australian consumers;**
- **an 'intelligence hub' that facilitates information sharing within and across industry sectors and provides:**
  - ⇒ **longer term analysis on cyber crime methodologies across a range of cyber crime types;**
  - ⇒ **education on the preservation of digital evidence; and**
  - ⇒ **support to law enforcement agencies for targeted prosecutions in Australia and overseas.**