1

Introduction

1.1 The Internet has developed rapidly over the past three decades, evolving from its military and academic origins to become a critical part of the communications infrastructure of most modern economies. It has brought with it a transformation in global communications, delivering new opportunities for business, service delivery, information sharing and communications. However, alongside these great benefits are new threats as cyber criminals exploit the weaknesses, complexity, speed and global scale of cyber space.

1.2 The nature of cyber crime has also undergone a transformation. The cyber criminal is no longer the nuisance hacker, motivated by the desire to show off their technical prowess, but more likely to be part of a loosely linked network of hackers, middlemen and organised crime who combine to commit large scale online crimes for significant profit. Cyber crime is now a sophisticated transnational threat that operates on an industrial scale and has become an increasingly important issue for the global community.

1.3 This inquiry is a timely adjunct to three major e-security policy reviews undertaken by the US, the UK and Australia in the past 18 months. In June 2009 the White House released the *Cyber Space Policy Review*,[1] the UK published *Digital Britain* and subsequently released the *Cyber Security Strategy of the United Kingdom* also in June 2009.[2] In Australia, an *E Security Review,* announced in early 2008, culminated in the release of the Australian Government's *Cyber Security Strategy* on 23 November 2009.[3]

---

1 *Cyber Space Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure*, White House, 29 May 2009.

2 *Cyber Security Strategy of the United Kingdom: safety, security and resilience in cyber space*, Cabinet Office (UK), June 2009.

3 *Cyber Security Strategy*, Australian Government, 2009.

1.4 These reviews reflect the importance that governments of the developed economies attach to e-security as a national and international issue. The need for a more integrated and coherent policy response to the realities of cyber space has been recognised by the US, the UK and Australia. However, many of the responses to new cyber threats have been driven by national security concerns and the need to protect critical public infrastructure. While these are important national objectives, this inquiry was concerned with the incidence and impacts of a range of cyber crime types that affect Australian society more generally.

1.5 It is not the first Parliamentary investigation into the wider impacts of this problem. In 2004, the Parliamentary Joint Committee on the Australian Crime Commission (ACC) inquired into ACC's role in relation to cyber crime.[4] In the same year, the Victorian Parliament examined the problem of fraud in the context of e-commerce.[5] More recently, personal Internet security was the subject of an inquiry by the UK House of Lords Science and Technology Committee.[6]

Referral of the Inquiry

1.6 On 13 May 2009, Senator the Hon Stephen Conroy, Minister for Broadband, Communications and the Digital Economy (DBCDE) wrote to the House of Representatives Standing Committee on Communications (the Committee) asking it to inquire into the incidence and impact of cyber crime on consumers and the Australian economy, and examine the adequacy of Australia's measures to combat the problem.

1.7 The terms of reference are set out at the front of this report.

1.8 A media release announcing the inquiry was issued on 18 May 2009 and published on the Committee's website on the same day. The terms of reference were advertised and written submissions invited in *The Australian* on 27 May and 10 June 2009. The inquiry was also advertised in the July issue of *Net Guide* and *Australian PC*.

1.9 The Committee wrote to over two hundred stakeholders encompassing government departments, regulatory agencies, consumer groups, IT vendors, banks and credit unions, peak industry bodies, professional

4 Parliamentary Joint Committee on the Australian Crime Commission, *Cybercrime,* The Parliament of the Commonwealth of Australia, March 2004.

5 Drug and Crime Prevention Committee, *Final Report of the Inquiry into Fraud and Electronic Commerce*, Parliament of Victoria, January 2004.

6 Science and Technology Committee, *Personal Internet Security*, Volume 1 Report, House of Lords, August 2007.

associations, academics and researchers. These invitations included relevant overseas bodies.

1.10 Written submissions were received from sixty-eight organisations and individuals. The list of submissions appears as Appendix A. The Committee also accepted twenty-two exhibits. The list of exhibits appears as Appendix B.

1.11 Fifty-three witnesses appeared in person to give oral evidence during eleven separate hearings in Canberra and Sydney between August 2009 and March 2010, and several witnesses provided additional evidence in response to questions on notice. The list of witnesses appears as Appendix C. The Committee also conducted an inspection of the Australian Federal Police high tech crime facilities in Canberra on 23 November 2009.

Definition of Cyber Crime

1.12 The Committee had to consider the scope of the inquiry and, in particular, the meaning of 'cyber crime' in the context of the terms of reference. The *Cyber Security Strategy* defines 'cyber crime' as offences against computers and computer systems, such as hacking, malware intrusions, and denial of service attacks. However, it quickly became apparent that terms such as 'cyber crime', 'technology enabled crime', 'Internet crime', 'e-crime', and 'online crime' are used interchangeably across government agencies and the community. Given the complex and interlinked nature of criminal activity it was important not to be artificially limited by a narrow technical definition of cyber crime. The Committee has used 'cyber crime' in its wider sense to include both offences against computers and computer systems and technology enabled crime.

1.13 Some witnesses also made a distinction between 'e-security' and 'cyber safety', especially where the latter involved children and young people in conduct that is not generally characterised as e-crime. The Committee did not entirely accept the distinction. However, the evidence on the problems of cyber bullying, stalking, and the unauthorised publication of damaging, images, was limited. The Committee did not seek out evidence on online child sex exploitation or the online publication of pornography because, although this is an aspect of cyber crime, it has been dealt with extensively by the Parliament.

1.14 Finally, in March 2010 the Parliament established a Joint Select Committee on Cyber Safety to take a more in depth look at these related areas of online conduct, especially as they relate to children and young people. Consequently, while the Committee is concerned about the exposure of

children and young people to online exploitation and the misuse of new social media, this was not the focus of this inquiry.

Overview of the Report

1.15 There was a clear message to the Committee that home users are most vulnerable to cyber crime, often unwittingly exposing themselves and others to e-security risks through a lack of online protections. While prevention through education is important, on its own education is insufficient to combat sophisticated cyber crime techniques. The Committee believes that it is time to shift our thinking toward a model where consumers, industry and government accept greater shared responsibility for personal Internet security.

1.16 In overview, the following three chapters that explain the complex nature of cybercrime, the need for comprehensive research to support policy development and the gap between end user awareness and preventative action. The remaining seven chapters that discuss proposals to strengthen Australia's response by committing to a more integrated, coordinated and concerted effort to target both policy and law enforcement against cyber criminals.

1.17 Chapter 2 examines the nature, prevalence and economic impact of cyber crime. It explains the role of botnets, which provide the infrastructure from which most criminal activity is launched. Cyber crime is often a combination of activities such as malware, spam, phishing, and spyware and it can be difficult to separate the civil and criminal aspects. These techniques are used to steal vast quantities of personal and financial information for sale in the underground market and for use for financial and identity crimes. While anti-virus software and cautious online behaviour can reduce e-security risks many viruses and other criminal techniques are undetectable.

1.18 The need for data collection and research as a necessary pre-requisite to effective policy development is canvassed in Chapter 3. The evidence from Information Technology (IT) security companies shows an exponential growth in malware and related computer offences. Under reporting of computer offences and online identity and financial crimes makes it difficult to measure the scope of the problem. Other cyber crime types, such as fraudulent websites, romance scams and advance fee fraud, are also under reported often because the victims are too embarrassed to come forward.

1.19 Chapter 4 describes the current level of public awareness of e-security threats and the vulnerability of Australian end users. The evidence indicates that even high levels of awareness do not necessarily translate into preventative action. Surveys indicate that only about half of the end users connected to the Internet have installed anti-virus software and many do not update their software.[7] And, despite efforts by government agencies and the banking industry, the Australian Bureau of Statistics has estimated that in 2006 alone 30,400 Australians were a victim of an online phishing scam.[8]

1.20 It is against this background that the remaining chapters of the report discuss proposals for a more integrated, coordinated and concerted approach to the problem of cyber crime as it impacts on consumers and business.

1.21 The theme of Chapter 5 is coordination across government, law enforcement authorities and between the public and private sector. There is a plethora of government agencies and private stakeholders, including Internet Service Providers (ISPs), Domain Name Registrars as well as the IT industry, with some role in relation to cyber crime. The Committee believes that, to get a more strategic approach to policy and better overall coordination, the Commonwealth needs to take more of a leadership role. In particular, all Australians would benefit from a national point of coordination and oversight of a broader national cyberspace strategy.

1.22 The transnational nature of cyber crime also means that Australian law enforcement efforts need more strategic and nationally scaled coordination. The Committee has recommended a one stop shop national centre for reporting a range of cyber crime types. This would give the public a single point of entry to report cyber crime. It would allow for the handling at first instance of both civil and criminal matters, and the collection and aggregation of intelligence data so that investigators can see the bigger picture.

1.23 Chapter 5 also discusses real time information sharing and an 'intelligence hub' to promote intelligence sharing and better trend analysis. The aim is to move the existing public-private information sharing beyond national security threats to include a wider range of cyber crime types.

---

7 Australian Communications and Media Authority, *Australia in the Digital Economy: Trust and Confidence*, ACMA, March 2009, p.39; AusCERT, *AusCERT Home Users Computer Security Survey 2008*, AusCERT, 2008, p.3.

8 Australian Bureau of Statistics, *2007 Personal Fraud Survey, ABS Catalogue No 4528.0,* ABS, 2007, p. 21.

1.24 Chapter 6 outlines the existing criminal law relating to computer offences and identity fraud, and it briefly canvasses some aspects of law enforcement powers. The chapter concludes that the legal framework has undergone significant development, although there continues to be a problem of lack of uniformity. The Australian Government should also expedite its work to bring domestic laws into conformity with the Council of Europe Convention on Cybercrime and seek accession to the treaty as soon as possible. This is important to strengthen Australia's international cooperation and to show leadership in the Asia Pacific Region.

1.25 Chapter 7 looks at the role of public and commercial stakeholders in protecting the integrity of the Internet. As previously stated, the Committee believes that protecting the integrity of the Internet is a shared responsibility, between government, private sector stakeholders, and end users. To translate this philosophy into concrete action the government should work with industry to do four key things:

- develop the voluntary *E Security Code of Practice* for ISPs into a more comprehensive document and register it as a mandatory code under the *Telecommunications Act 1997* (Cth);
- require Domain Name Registrars and Resellers should be required to apply a 'know your customer' principle to reduce the fraudulent use of domain names;
- build on the Australian Internet Security Initiative to implement a more integrated scheme to detect botnets and remediate compromised computers operating across Australian networks;
- fund the Australian Communications and Media Authority (ACMA) to detect compromised websites and empower ACMA to order the temporary or permanent removal of fraudulent or compromised websites from the Australian Internet.

1.26 Chapter 8 looks at the consumer protection regime, and how it applies to cyber crime. The new *Australian Consumer Law* strengthens the enforcement powers of the Australian Competition and Consumer Commission to protect consumers. The Committee believes there should be a specific consumer law requirement for informed consent before software programs are downloaded.

1.27 The new framework also provides an opportunity to develop national information standards for IT vendors and retailers to provide consistent e-security information to consumers. This should be aimed at encouraging consumers to take preventative steps and ensure they are better informed about the e-security risks of the IT products they are buying. The issue of

IT vendor liability is discussed, and a more in depth investigation by the Productivity Commission is recommended. The Committee has also recommended that the IT industry adopt better design standards for prompting consumers to adopt stronger security settings.

1.28 Chapter 9 discusses privacy law protections and endorses many of the recommendations of the Australian Law Reform Commission that relate to privacy and new technologies. In particular, the Committee supports the mandatory reporting of data breaches to ensure that individuals are able to take steps to protect themselves.

1.29 Chapter 10 addresses the adequacy of community education and awareness raising initiatives. A great deal of effort is expended in communicating e-security messages to the population: to young people and their parents through the schools, to adult consumers via the banking industry and the Australian Consumer Fraud Task Force. The Committee heard that the DBCDE's *Cyber Security Awareness Week* will move onto a more continuous footing with initiatives throughout the year. The value of promoting IT literacy generally, as distinct from for purely vocational purposes, was also advocated.

1.30 Despite these efforts Australia still has a long way to go to achieve the kind of cultural change necessary to make the population more e-security aware and active. There is an important role here for a clearly articulated national cyber security community education strategy, that identifies the different target audiences and education and information strategies to reach those audiences. Such a strategy should include a broad based 'public health style' campaign to promote key e-security messages in simple and easy to understand language. The DBCDE is best placed to develop a national cyber security education strategy, which should be reported on annually to the Parliament.

1.31 The final chapter, Chapter 11, canvasses evidence of new and emerging technologies with e-security features. The Committee concludes that, while technology alone will not solve the problem of cyber crime, continued technological innovation is needed to meet new and evolving threats. The Committee concludes that the value of such technologies to mitigating cyber crime should be considered, and that a competitive and innovative IT security industry should be maintained. This does not,

however, prevent better security standards becoming a higher priority for IT vendors.