Parliament of Australia
Department of Parliamentary Services

Parliamentary Library
Information, analysis and advice for the Parliament

BACKGROUND NOTE

www.aph.gov.au/library

24 February 2010, 2009–10

Cyber Crime 2.0 versus the Twittering classes

Matthew L James
Science, Technology, Environment and Resources Section

Contents

Glossary

Blog	a web log website, usually maintained by an individual with regular entries of commentary, descriptions of events, or other material such as graphics or video.
Bot	autonomous 'robot' software that operates covertly for a computer user or program.
Botnet	computer 'robots' acting as a network of computers on the internet that, although their users are unaware of it, have been compromised to transmit to other computers.
CERT	Computer Emergency Response Team on cyber security information.
Cyber crime	an array of criminal activity including offences against computer data and systems, computer-related offences, content offences, and copyright offences.
Cyber security/computer security	information security applied to computers and networks.
Cyber space	a virtual environment of information and interactions between computer users.
DDoS	Distributed Denial of Service, which attempts to make a computer resource unavailable.
Firewall	software programs that protect the resources of a private computer or network from users from other networks.
ICT	Information and Communica tion(s) Technology as used in its widest sense.
IM	Instant Messaging is a form of real-time communication between two or more people based on typed text, conveyed via devices connected over a network such as the internet.
Malware	malicious software designed to infiltrate or damage a computer system.
Phishing	a social engineering technique of attempting to acquire sensitive information such as usernames, passwords and financial details by masquerading as a trustworthy entity.
P2P	Peer to Peer distributed computer network architecture that facilitates communications.
RSS	Really Simple Syndication news feeds that advise of changes in information content.
Social engineering	is the act of manipulating people into performing actions or divulging confidential information; in this context through the use of computers and the internet.
Trojans	non-self-replicating malware that appears to perform a desirable function for the user but instead facilitates unauthorized access to the user's computer system.
Virus	software designed to cause undesirable effects on computer systems.
VoIP	Voice over Internet Protocol – a type of transmission technology for delivery of voice communications over networks such as the internet or other packet-switched networks.
Web 2.0	internet applications that facilitate interactive information sharing, interoperability, user-centred design and collaboration.
Zombie	a computer that has been infected with a virus or daemon that places that computer under the control of a malicious hacker without the knowledge of the owner of the computer.

Major Issues

This paper contends that the hype surrounding the steep rise of social media networking website use has tended to mask the reality of a corresponding growth in online fraud and crime. New Web 2.0 technologies may enable inventive interactivity online, but they also foster innovative ways for those intent on nefarious means to achieve their ends.

Newly popular social media are a case in point where even the short trivia uttered by 'the masses' can be used online by less community-minded types to access information for purposes such as identity theft and other online-based crimes. From social engineering techniques to 'botnets', their means to pursue anti-social activity are many and growing. Social media is just one possible target/infection vector. Nonetheless, the social media have been very popular and successful of late.

This paper provides a general review of cyber security issues for which the social media is one possible target for criminal activity that is not just purely online, but can become physical as well. For instance, social media sites such as Twitter may be used by thieves to find out when users are away from home in order to break into houses.

The range of threats is not just malicious software import, but information gathering and surveillance, together with identity theft. Personal emails, Instant Messaging, and mobile Short Message Service/Multimedia Message Service may also be quite significant areas of cyber crime.

In response to such developments, Australian Government agencies have been marshalled to meet the threat but a very significant challenge exists in how to deal with it effectively across many different portfolios such as defence and communications. This paper outlines current policy approaches in Australia and overseas to address the online security issue, such as the new National Cyber Security Strategy here that operates within international strategies.

This paper does not cover matters of cyber safety, cyber bullying, unsafe online behaviour or issues of privacy, content and copyright. The paper does however have a focus on the regulation of rapidly changing technology developments found online.

The Participatory Internet: Web 2.0

The internet provided new possibilities in personal communication, with the first generation internet "Web 1.0" enabling broadcast, point to point and hub and spoke communication activity through websites. The second generation, evolving as "Web 2.0", enables different connections and collaborations with an interactive and social emphasis.

A fundamental function of social networking sites is that they are interactive so that site owners and visitors collaborate on the content. The rapid expansion of social media is

fuelling developments in social networking, a rise of new media influences, and the personalisation of web experiences, including location-based services.

Web 2.0 is thus a generic term currently used to describe interactive ways of participating on the Internet, with a focus on the social nature of the internet and on personal interactions and social networking applications, such as via:

- Collecting Intelligence—through wikis or web pages and intranets aggregating content, such as the free online Wikipedia collaborative information compendium,[1]
- Information Tagging—of maps, data, such as Open Australia.org,[2]
- Social networking—sites such as MySpace, Facebook, Twitter, Bebo and LinkedIn[3]
- User generated multimedia—on YouTube, Twitter and some news sites like Crikey,[4]
- Ideas Fora—'Australia 2020', and surveys on news sites, etc., and[5]
- Citizens' participation and electronic democracy—GetUp!, newdemocracy, Australian eDemocracy sites.[6]

Politicians are also using social networking sites as part of awareness campaigns and for fundraising purposes.[7] Facebook and MySpace are being used to engage and recruit new members and supporters to such sites. Facebook now has over 350 million users and LinkedIn over 34 million, with many other such sites available for online users to access.

In January 2009, the United Kingdom Parliamentary Office of Science and Technology commented on Web2.0 and electronic democracy (e-Democracy) that:

---

1. Wikipedia website, viewed 19 February 2010, http://www.wikipedia.org.
2. Open Australia website, viewed 15 September 2009, http://www.openaustralia.org/.
3. MySpace website, viewed 19 February 2010, http://www.myspace.com, Facebook website, viewed 19 February 2010, http://www.facebook.com, Twitter website, viewed 19 February 2010, http://twitter.com, Bebo website, viewed 20 February 2010, http://www.bebo.com, LinkedIn website, viewed 20 February 2010, http://www.linkedin.com.
4. YouTube website, viewed 19 February 2010, http://www.youtube.com, Crikey website, viewed 19 February 2010, http://www.crikey.com.au.
5. Australia 2020 website, viewed 19 February 2010, http://www.australia2020.gov.au.
6. GetUp! website, viewed 15 September 2009, http://www.getup.org.au/, new democracy website, viewed 15 September 2009, http://newdemocracy.com.au/, Australian eDemocracy website, viewed 15 September 2009, http://democracy.nationalforum.com.au/.
7. M Read, 'Twittering Pollies', *The Adelaide Review*, August 2009, p. 20.

A variety of technologies can be used for e-Democracy, such as Interactive Digital Television and mobile phones. However, the most popular is the World Wide Web. In its early days the web focused on delivery of information, with the user as a passive consumer. However, 'Web 2.0' applications allow information sharing and peer-to-peer collaboration, for example:

- Blogs (or web-logs) which usually take the form of an online diary: such as the House of Lords' 'Lords of the Blog' at http://lordsoftheblog.wordpress.com. This is a pilot project of the Hansard Society aiming to encourage dialogue with the House of Lords.

- Social networking sites like Facebook and YouTube (used by ~11 million UK residents a month, about one third of all UK internet users) allow users to interact, and share images or audio/video clips. Almost 100 MPs have Facebook pages. Parliament and 10 Downing Street started their own YouTube channels in 2007. A key feature is the viral nature in which information and commentary can propagate rapidly across the network.[8]

Australia in the Web 2.0 Digital Economy

In August and September 2008, the Australian Government held consultations with industry and other stakeholders on the digital economy, in the Digital Economy Forum[9]. The Forum decided 'to collaborate to develop a road map for the future of the digital economy in Australia'[10]. This led to the development of a paper on the future directions of the digital economy, released in July 2009 that outlines an exciting future for such online trends.[11] An Australian Computer Society response to the Digital Economy paper provides a considered overarching opinion:

> There is a fundamental question around how the Government is going to ensure Australia is capable of prospering in a global economy that is digitally enabled. Many of our near neighbours and trading partners have developed national blueprints and manifestos with key

8. Parliamentary Office of Science and Technology (POST), 'e-Democracy', *postnote*, no. 132, January 2009, viewed 15 September 2009, http://www.parliament.uk/documents/upload/postpn321.pdf

9. Digital economy workshops and forum', Department of Broadband, Communications and the Digital Economy, viewed 23 September 2009, http://www.dbcde.gov.au/digital_economy/future_directions_of_the_digital_economy/digital_economy_workshops_and_forum

10. S Conroy (Minister for Broadband, Communications and the Digital Economy), *Industry, business & Government drive digital economy future*, media release, 10 September 2008, viewed 23 September 2009, http://www.minister.dbcde.gov.au/media/media_releases/2008/069

11. Department of Broadband, Communications and the Digital Economy, *Australia's digital economy*, Canberra, July 2009, viewed 15 September 2009, http://www.dbcde.gov.au/digital_economy/future_directions_of_the_digital_economy/australias_digital_economy_future_directions/final_report/australias_digital_economy.

> strategic goals and benchmarks that give priority to their digital economies and direction to their ICT industry sectors.
>
> Most recently the UK has released "Digital Britain" to highlight the importance of, and give focus and stimulus to, its digital economy. Australia must also, as a national priority, develop a comprehensive national digital economy strategy that addresses government activity, the development of digital resources, skills and industry competencies, and sets out a blueprint to enhance our engagement in the global digital economy.
>
> Without such a strategy, we are left with a series of well meaning but largely uncoordinated and unfocused Government reviews, activities and programs that do not reach their full potential. Through the NBN, the higher education review, the innovation review, the review of temporary migration, the Gershon review, the current review of our taxation system, the 2020 summit and consultation forums and workshops on the digital economy, Australia has or will have many of the fundamentals in place that it needs for a thriving digital economy. What we need now is leadership and direction to drive the digital economy forward.[12]

In March 2009, the Australian Communications and Media Authority (ACMA) released *Trends in Communications and Media Technology, Applications and Use*.[13] The report paints a rosy picture of the online future and also dwells on the rise of the social web. However some new emerging regulatory challenges that the report also identifies include:

- increasing interest from the public in data portability between web internet service providers (ISPs), and the management of online identity, data and reputation;
- the impact of evolving cyber-crime economies which operate across the internet incorporating data theft and fraud.

The ACMA report states that the types of crime alluded to here may include:

- malicious software (malware) threats from poorly designed and maintained web sites,
- botnet or malware delivery systems growing in sophistication and obfuscation ability,
- cyber warfare through the direct denial or service attacks by antagonistic nations, and

12. Australian Computer Society, *ACS response to the digital economy future direction consultation paper*, viewed 15 September 2009, http://www.acs.org.au/index.cfm?action=show&conID=200902110929590148.

13. Australian Communications and Media Authority (ACMA), *Trends in Communications and Media Technology, Applications and Use*, Canberra, March 2009, viewed 15 September 2009, http://www.acma.gov.au/WEB/STANDARD/pc=PC_311690.

- voice over internet protocol (VoIP) spam emails and data phishing (scanning).

Cyber Security Concerns

The matter of internet security or cyber security has recently reached the scientific literature. Frederick R. Chang from the Department of Computer Science at the University of Texas at Austin noted, in *Science* journal, that:

> Computers can be infected merely by surfing the Web. By attacking a single Web site, attackers can potentially infect the computers of all visitors to that site. Using a technique known as SQL (Structured Query Language) injection, an attacker can insert malicious code into the database associated with the Web Site. Using another technique, cross-site scripting,…users visiting legitimate Web sites were invisibly redirected to a server that downloaded malicious software onto the user's machine….Botnets are responsible for attacks including spam, phishing, distributed denial of service, data harvesting, click fraud and password cracking. A bot is a computer that has been infected such that it can be remotely controlled: a botnet is a large network of bots…. (Botnet) **Storm also made sophisticated use of social engineering techniques: it was highly effective at inducing people to take action (such as to download and execute files),** thereby infecting their computers with malware….A key problem is that too much software today is insecure….If security is to be built into the software: then the software must be free of known bugs that can be exploited to compromise security… Building security in is not a new problem. Fortunately, important technical advances over the past 25 years have improved the ability of developers to build more fundamentally secure systems. Technology advances alone will not solve all the problems. …**A key question is why social engineering techniques continue to be so successful. As technical measures improve the security of systems, the end-user will increasingly become the weakest link**.[14]

A less sanguine view on the reliability of computer software security appeared more recently from staff of the Department of Computer Science, University of Virginia, who contend that:

> The security model has remained the same since the 1960s, and software engineers have added more and more patches and widgets to try to enforce the security model. The complex interaction of this additional code with the extant code just provides more opportunities for security failures…We think,… rather, there should be a minimal central mechanism that enables implementation of many security policies in application code – systems attuned to the needs of differing applications and organizations….Incorporating multiple security policies and multiple implementations of the same policy can dramatically reduce this monoculture-induced vulnerability.[15]

14. F R Chang, 'Is your computer secure', *Science*, vol. 325, 31 July 2009, pp. 550–551.

15. W A Wolf and A E Jones, 'Reflections on cybersecurity', *Science,* vol. 326, 13 November 2009, pp. 943–944.

However we need to distinguish between those security events that occur as a direct result of software vulnerabilities and those physical criminal activities that result from online user actions and social engineering techniques. This paper provides merely an overview.

Government and Web 2.0

In 2009 the Australian Government launched a Gov 2.0 Taskforce to investigate how government can utilise new 'Web 2.0' approaches to improve engagement with citizens.[16] Under its terms of reference the Taskforce investigated how to make government information more accessible and usable, to further establish a pro-disclosure culture around non-sensitive Public Service information. The Taskforce was also expected to examine how to make government more consultative and transparent; how to build a culture of online innovation within government; and how to promote cross-agency collaboration in online and information initiatives. Some $2.45 million was allocated to the Gov 2.0 Taskforce to support development of Web 2.0 tools and applications.

The report of the Government 2.0 Taskforce was released on 20 December 2009. This report suggested that 'Government 2.0' might be understood as the application of tools and approaches associated with collaborative web or 'Web 2.0' as it is termed. The report said that these tools were potentially transformative of the way governments operate.[17]

Such new participatory uses of the Internet offer innovative ways for government agencies to reach and better serve future client focus. For instance, in the Parliamentary Library new publications are notified via RSS (Really Simple Syndication) feeds, Twitter, a newsletter to Senators and Members and other Parliamentary clients (*This Sitting Week*) and directly by library staff if they are aware of a particular Senator or Members' interest.[18] Indeed, according to the Parliamentary Librarian commenting on Gov 2.0 in late August 2009:

> The Government's proposed Freedom of Information legislation, including the establishment of a position of Information Commissioner, will place new obligations on government agencies to pro-actively publish information. It is hoped that these reforms will lead to an improvement in practice so that the requirement for information management plans in agencies and a commitment to online publication is seen as a genuine step towards more extensive, open government. However to achieve Gov 2.0, or indeed an effective Gov 1.0, more than mere words are required. We have seen a reduction in access to government information in the past two years in some areas. I encourage the Gov 2.0 Taskforce to go

16. Government 2.0 Taskforce website, viewed 15 September 2009, http://gov2.net.au/.

17. Government 2.0 Taskforce, *Engage: Getting on with Government 2.0*, Australian Government Information Management Office, Department of Finance and Deregulation, viewed 19 February 2010, http://www.finance.gov.au/publications/gov20taskforcereport/index.html.

18. Parliamentary Library website, viewed 20 February 2010, http://www.aph.gov.au/library/rssinfo.htm, Twitter Parliamentary Library website, viewed 20 February 2010, http://twitter.com/ParlLibrary.

> beyond the current restrictive practices of agencies to seek a long-term program of progressive opening up of information and government practices." [19]

The Twittering Classes

The latest social networking trend has to be Twitter, a blog host with postings limited to 140 characters.[20] Just as one can go to individual regular blogs, one can go to Twitter to read blog posts, or as they are known on Twitter, tweets. When one "follows" someone on Twitter, they are subscribing to a feed of these tweets, in the manner of an RSS feed. One can skim through what people are talking about, looking for anything interesting. A feature that differentiates Twitter from normal blogs is that one can see what Twitter feeds others are monitoring; but in the rest of the blog environment one cannot see the blogs that others are monitoring.

According to the Australian website information service Web Search Pacific, Twitter is starting to be a serious tool for researchers.[21] Twitter can be used to learn about new ideas and new resources, and to listen to what thought leaders have to say. And strategic tweeters, just like strategic bloggers, understand that their success may lie in sharing thoughtful comments and insights into their industry. Blogs encourage participation by allowing readers to comment on their blog posts, thereby creating a community discussion around a topic. Likewise, Twitter has a number of features that let readers interact with the "tweetosphere". Readers can respond to a tweet or can forward it on to their followers ("re-tweet") a Twitter message they find useful, just as they would link to it in a blog post.

But is this all just hype bordering on voyeurism? In June 2009 a web analytics firm Hub Spot reportedly found that some 55 per cent of the then 6 million Twitter members had never actually sent a text message.[22] As well, some 10 per cent of Twitter users accounted then for 90 per cent of all tweet traffic. Nonetheless, journalists, politicians and the public use Twitter.

Indeed, an Australian Computer Society magazine article 'Why you should Twitter', outlines some benefits to business from encouraging involvement with customers to build an online presence, protecting brands and staying ahead of the game. [23] The article also notes the risks of receiving negative feedback online, falling behind and under-resourcing. ICT professionals are using social networks for customer service and marketing and keeping up with industry developments. For example, by monitoring Twitter feeds from their customers, ISP operators can respond to service complaints. Equally they can share tips on a common topic.

---

19. Parliamentary Library, *Library Update*, no. 34/09, 28 August 2009
20. Twitter website, viewed 15 September 2009, http://twitter.com/.
21. Web Search Pacific website, viewed 15 September 2009, http://www.websearchpacific.com/.
22. Hub Spot website, viewed 15 September 2009, http://www.hubspot.com/.
23. K Milesi and N Civins, 'Why you should Twitter', *Information Age*, Australian Computer Society, August/September 2009, pp. 43–45.

Cyber Storm Clouds Gather

The rise of interest in 'social media' and Web 2.0 has seen claims made on its usefulness and idleness. Some businesses see social marketing as disruptive and without controls, while others use social networks to source collaborators, sound off ideas and raise their profiles.

So the users of social network sites are blurring boundaries between personal and professional online activities and management controls. However, placing personal details online enables less community-minded types to access information for other purposes such as identity theft and other online based crimes. Equally though, police and authorities can use social networking sites to monitor illegal activities.

There many are other security aspects to consider such as privacy, confidentiality and legal obligations thereto, which are not considered further in this particular paper. Note that this paper does not consider matters of cyber bullying and unsafe online behaviour. The Web 2.0 Taskforce Issues Paper does note the following in regards to security for online government:

> In comparison to many large commercial enterprises, public sector agencies in the main adopt quite restrictive practices in allowing staff access to Web 2.0 tools, social networking sites and even webmail. Most agencies simply ban access to these sites. One of the reasons often used to justify this position is the need to protect internal IT systems from exposure to threats from the internet. Highly prescriptive and centrally mandated security policies are often rigorously applied. Given the low risk culture of the public sector, it is difficult to see how agencies wishing to enter into the Web 2.0 world will be able to argue that the benefits to citizens, and to the operations of the agency, are of sufficient value to offset an exposure which cannot easily be assessed. Clearly the risks to agencies will vary depending on the nature of their business. It is unlikely that technology alone will solve this challenge. [24]

According to the Federal Government's Stay Smart Online website:

> People use social networking sites such as MySpace, Facebook, Bebo, Twitter and Linkedin for many reasons. People use them to stay in touch with friends, make new friends or business connections and to share information and opinions about a range of topics. These sites let you share your personal information and opinions in profiles, updates, forums, chat rooms, email and instant messaging tools.
>
> **However, you need to be careful about the information that you share on these sites and how you protect it.** While the majority of people using these sites are not threatening, people can use your information to embarrass you or damage your reputation. **Criminals can use your information to steal your identity.**[25]

24. Government 2.0 Taskforce, *Issues Paper*, clause 225, viewed 15 September 2009, http://gov2.net.au/consultation/2009/07/23/towards-government-2-0-an-issues-paper-final/.

25. Australian Government, Stay Smart Online: Social Networking Website, viewed 15 September 2009, http://www.staysmartonline.gov.au/smart-online/social-networking.

Stay Smart Online and Cyber Smart provide an overview of some cyber crime scenarios.[26]

Phishing

Phishing emails (pronounced *fishing*) are fraudulent email messages used to gain access to personal information for illegal purposes, such as transferring funds or purchasing goods. These fraudulent messages appear to come from legitimate businesses such as banks and other financial institutions….They are designed to trick people into disclosing personal data such as bank account details, passwords or credit card numbers.

Social Networking

These let users share personal information and opinions in profiles, updates, forums, chat rooms, email and instant messaging tools. However, users need to be careful about the information that they share on these sites and how they protect it. While the majority of people using these sites are not threatening, people can use information to embarrass you or damage your reputation. Criminals can use your information to steal your identity.

Malware

Anti-virus software helps prevent infections from a wide range of malicious software (also called malware). Malware can be transmitted by downloading infected programs from websites or clicking on a web link in an email. Computer malware is a serious threat.

Smartphones and Multimedia Messages

Advanced capabilities such as Bluetooth also mean that there is an increased risk that private information on the phone could be stolen, or the phone could become infected by malicious software. In addition, if a phone is lost or stolen, personal information including passwords, banking details, emails and photos could be used unlawfully.

Multimedia messages or attachments in emails could contain malicious software or take users to a malicious website. Users should not download content such as applications from an unknown or unreliable source. They could contain malicious software.

Virus and anti-virus

A virus is a computer program that is designed to cause undesirable effects on computer systems. Viruses are often disguised as something else so that they can be transferred from one computer to another without the users knowing. They can be hidden in emails, on CDs or in files that are shared across the internet. Computer viruses can cause harm to computer systems and need to be avoided.

---

26. Department of Broadband, Communications and the Digital Economy *Stay Smart Online* website, viewed 20 February 2010, http://www.staysmartonline.gov.au/smart-online, Australian Communications and Media Authority, Cybersmart website, viewed 20 February 2010, http://www.cybersmart.gov.au/.

Attack of the Zombie Botnets

Overnight on 9 September 2009, the Prime Minister's website suffered a distributed denial of service (DDoS) attack that rendered inoperable both it and the site of the Australian Communications and Media Authority. In this instance the attack was said to be in protest at government plans to filter the Internet.[27] While dismissed as a juvenile attack, it showed that service bans can occur. Earlier the same day, the Australian Federal Police Commander told parliamentarians that security must be at the centre of the proposed new National Broadband Network.[28]

Other examples of social networking actions with a clear political intent are relevant here. Following Iran's disputed presidential election, activists distributed Twitter messages to alert the world to their alleged plight, while a few months earlier, Moldavian campaigners used Facebook to organise anti-government protests. In response to such activities, political filtering grew, while at times entire social networking services became unavailable in certain countries.[29] But there are other dangers with social media:

> **A new hacking incident report warns there has been a steep rise in attacks at social-networking hotspots including wildly popular micro-blogging service Twitter**. Hackers aren't just hunting for victims in the flocks of people at social networks; they're also using Twitter to command "botnet" armies of infected computers, according to Internet security specialists.
>
> "Any website with a huge user following is now attracting the bad guys," said Ryan Barnett, director of application security research for Breach Security. "A lot of Web 2.0 widgets, mashups and the like that users go for make it easy for all these guys to launch attacks."
>
> Facebook became an Internet star after opening its platform to widgets, mini-applications made by outside developers, and now boasts more than 250 million members. Barnett was among the authors of a Web Hacking Incidents Database Bi-Annual Report that concluded social-networking was the most popular "vertical market" for hackers in the first six months

27. T Lohman, 'PM's site suffers Anonymous DDos attack', *Computerworld*, 10 September 2009, viewed 19 February 2010, http://www.computerworld.com.au/article/318011/pm_site_suffers_anonymous_ddos_attack/.
28. House of Representatives, Standing Committee on Communications, Inquiry into Cyber Crime, Public Hearing Transcript 9 September 2009, viewed 15 September 2009, http://www.aph.gov.au/house/committee/coms/cybercrime/hearings/program02.pdf.
29. J Giles, 'Worldwide battle for control of the internet', *New Scientist*, 22 August 2009, pp. 18–19.

> of this year. The prime targets for attacks in 2008 were government and law enforcement websites, according to the Web Hacking Incidents Database. [30]

Cyber Crime

With a strong background in cyber safety, in both the private and public sectors, Mr Alastair MacGibbon has written an Australian Strategic Policy Institute *Special Report* on cyber security: Threats and responses in the information age.[31] MacGibbon writes most forcefully on the risks that we all face in the online environment and is eloquent in calling for strong government and business security actions. He notes that there are three layers of ICT systems, namely government, business and citizen but users can't identify which type they linked to and as a consequence security had to focus on the individual.

Online activity has principally been driven by anonymity, he believes, with 1 billion people now surfing the web. However a surprising half of online Australians have no up-to-date firewall or anti-virus protection, a statistic sure to shock intending vendors of the proposed National Broadband Network. Especially when considering the new social media:

> Oftentimes such malware is combined with 'social engineering', aimed at convincing users to undertake activities they otherwise would not. It is this amalgam of devious software and human trickery which has compounded the problem, multiplying the vectors of attack and making it much harder to reduce risk.[32]

MacGibbon states that the growth in malware and phishing of personal data since 2003, plus later social engineering techniques, has not seen corresponding security actions. Centralised computer systems also face attack with exploitation and government espionage as real threats with cyber warfare implications, he says. He states that as yet there has been no online terrorist attack, but we might expect one given the advantages it offers to the culprits in terms of anonymity, scale and propaganda value. Further he notes that:

> We argue, too, that industry self-regulation has failed in the cyber security space. The paper calls for national leadership where prompt but considered decisions are arrived at in partnership with industry…. In short, cyber security is a growing national security concern for three main reasons: the threat posed to Australia's economic interests; the integrity of

30. G Chapman, 'Cyber crooks riding social-networking wave: report', *Sydney Morning Herald*, August 18 2009, viewed 15 September 2009, http://news.smh.com.au/breaking-news-technology/cyber-crooks-riding-socialnetworking-wave-report-20090818-eofj.html.

31. A MacGibbon, 'Cyber security: Threats and responses in the information age', Australian Strategic Policy Institute, *Special Report*, Issue 25, Canberra, December 2009, viewed 19 February 2010, http://www.aspi.org.au/publications/publication_details.aspx?ContentID=233&pubtype=10.

32. Ibid.

> Australian Government information and systems; and the wellbeing of the Australian public.[33]

The Australian computer industry notes:

> Keeping up with malware signatures is becoming unsustainable. In 2008, for example, Symantec put out more antivirus signatures than it did in the company's previous 17 years of existence. Ultimately, the only answer to the increasing proliferation and sophistication of malware may be whitelisting, where the only executable (program files) that can run on a system are known, good executables.[34]

In April 2009, the anti-virus vendor Symantec released its *Global Internet Security Threat Report* finding that credit card information, bank account credentials, email login details and full identities are readily available at cheap prices to anyone willing to pay.[35] Still it may be argued that such members of the computer industry could exaggerate the crime threat. To examine this, in May 2009, the Minister for Broadband Communications and the Digital Economy Senator the Hon Stephen Conroy referred an inquiry into Cyber Crime to the House of Representatives Standing Committee on Communications.[36] The Australian Information Industry Association submission to the Inquiry provides a clarification of cyber crime:

> Cyber crime can be understood by reference to its eco-environment, cyberspace. The US has defined cyberspace as "the interdependent network of information technology infrastructures, and includes the internet, telecommunications networks, computer systems and embedded processors and controllers in critical industries. Common usage of the term also refers to the virtual environment of information and interactions between people." By this definition, cyberspace is *not just the internet*; so cyber crime can occur in a much wider environment than the internet.[37]

The Australian Competition and Consumer Commission submission elaborates further:

> Cyber crimes are generally technology enabled and can involve significant potential social harm such as child pornography and cyber stalking or economic harm including frauds,

---

33. Ibid.

34. 'Top 10 emerging technologies', *Information Age*, Australian Computer Society, December 2009/January 2010, pp. 23–27.

35. Symantec website, viewed 15 September 2009, http://www.symantec.com/index.jsp.

36. House of Representatives, Standing Committee on Communications, Inquiry into Cyber Crime, Terms of Reference 13 May 2009, viewed 15 September 2009, http://www.aph.gov.au/house/committee/coms/cybercrime/tor.htm.

37. Australian Information Industry Association, *The incidence of cyber crime in Australia and its impact on consumers*, Submission to the House of Representatives, Standing Committee on Communications, Inquiry into Cyber Crime, June 2009, viewed 15 September 2009, http://www.aph.gov.au/house/committee/coms/cybercrime/subs/sub22.pdf.

> scams, spam, phishing and identity theft. The conduct may involve a number of perpetrators and in some cases, the perpetrator may not be aware of their involvement in the conduct.[38]

The Global Cyber Threat

The Australian Security and Intelligence Organisation (ASIO) notes that:

> Cyber threats are becoming more wide ranging, increasingly sophisticated (not only involving Trojans and malicious code, but also using social engineering techniques) and increasing in intensity. The perpetrators of such attacks can range from the ubiquitous hacker through to criminals, issue-motivated groups, terrorist organisations and nations. [39]

Illegal activities such as identity theft, financial fraud and malicious software now threaten individual privacy rights and business competitiveness, according to the Organisation for Economic Cooperation and Development (OECD).[40]

The Australian Federal Police submission to the cyber crime Inquiry says that:

> Major vulnerabilities in the current online environment centre around three key elements:
> 1. Lack of awareness of threats and human susceptibility to social engineering;
> 2. The exponential growth in malware; and
> 3. Problems with web architecture and security which leave sites and systems vulnerable….
>
> Investigations undertaken by the Australian Federal Police (AFP) have identified DDoS (Distributed Denial of Service) attacks committed by botnets containing more than 100,000 compromised computers across more than 120 countries. The ability of law enforcement to investigate and prosecute individuals behind such attacks is often thwarted by the trans-national nature of the Botnet make up and control systems.[41]

On social networking for example, from a leading American based internet security software corporation, the McAffee submission to the cyber crime Inquiry says:

---

38. Australian Competition and Consumer Commission, Submission to the House of Representatives, Standing Committee on Communications, Inquiry into Cyber Crime, July 2009, viewed 15 September 2009, http://www.aph.gov.au/house/committee/coms/cybercrime/subs/sub46.pdf.

39 Australian Security Intelligence Organisation (ASIO) Submission to the House of Representatives, Standing Committee on Communications, Inquiry into Cyber Crime, June 2009, viewed 15 September 2009, http://www.aph.gov.au/house/committee/coms/cybercrime/subs/sub47.pdf.

40. OECD, *Computer Viruses and Other Malicious Software: A Threat to the Internet Economy*, Organisation for Economic Cooperation and Development, March 2009, viewed 15 September 2009, http://www.oecd.org/document/16/0,3343,en_2649_34223_42276816_1_1_1_1,00.html.

41. Australian Federal Police (AFP) Submission to the House of Representatives, Standing Committee on Communications, Inquiry into Cyber Crime, June 2009, viewed 15 September 2009, http://www.aph.gov.au/house/committee/coms/cybercrime/subs/sub25.pdf.

> The growth in social networking and the implicit trust in these communities has given rise to new threat vectors in places like Facebook, Twitter and YouTube. Facebook and other social networking sites do not vet the community's shared programs for security issues, while Twitter and others have been plagued by a number of issues. Within these communities, threats now travel faster due to the enormous amount of trust their users place in one another. Because these web 2.0 generation of applications and websites provide enormous value to their user base, it is important to embrace them while also determining the best way to ensure these communities improve their safety for online users, and that the users themselves understand the implications. As when societies begin relying upon email in earnest, and virus education began in earnest, a similar urgent level of education is necessary for the use of web 2.0. [42]

In its submission to the Inquiry, global e-security provider Symantec notes that:

> E-security is a complex topic and there is a wide variety of risks. These risks could include loss or theft of personal information, targeted attacks using such personal information to further compromise the user, phishing attacks to obtain passwords for financial gain, denial-of-service (DoS) attacks on corporate systems causing loss of productivity and critical data, malicious attacks on industrial control systems, and in some cases distributed denial-of-service (DDoS) attacks targeting the national information infrastructure of an entire nation as we have seen in the case of Estonia or Georgia.
>
> More than ever, cyber criminals are presented with a wide range of possibilities to conduct such attacks. Widely-adopted technologies such as Instant Messaging (IM), VoIP, P2P and Web 2.0 are increasingly attractive platforms for attacks. For example, IM, one of the most successful and widely deployed applications on the Internet, has become a potent means to propagate viruses, worms and other threats. It is also particularly well suited for social engineering tactics being as it is a tool which tends to be inherently trusted by users….
>
> In this way, a popular, trusted site with a large number of visitors can yield thousands of compromises from a single attack, thus providing an optimal beachhead for distributing malicious code….
>
> Bots and bot networks are clearly a huge problem with significant impact to the wider economy. Bots are programs that are covertly installed on a targeted system, allowing an unauthorized user to remotely control the computer for a wide variety of purposes. Attackers often coordinate large groups of bot-controlled systems, or bot networks, to scan for vulnerable systems and use them to increase the speed and breadth of their attacks by launching coordinated attacks. [43]

---

42. McAfee Submission to the House of Representatives, Standing Committee on Communications, Inquiry into Cyber Crime, July 2009, viewed 15 September 2009, http://www.aph.gov.au/house/committee/coms/cybercrime/subs/sub10.pdf.

43. Symantec Submission to the House of Representatives, Standing Committee on Communications, Inquiry into Cyber Crime, July 2009, viewed 15 September 2009, http://www.aph.gov.au/house/committee/coms/cybercrime/subs/sub32.pdf.

Privacy and date breach disclosure requirements are other factors not covered here in this paper that focuses on cyber crime and security policy. There are though wider ramifications to consider in formulating e-security policies. There is a need to balance ICT security, performance and privacy, by engaging all stakeholders, but security is also a technical issue and not one to be just left to policy makers. For example, the various techniques of risk analysis used in security assessment have weaknesses and vulnerabilities not necessarily evident to policy makers.

Cyber Crime Risk Analysis

The sobering reality facing our efforts to fight cyber crime have been well documented lately:

> Banks, carriers and police have delivered a withering assessment of Australia's bid to combat cybercrime, warning federal politicians that efforts by dozens of government agencies to control the online scourge remain disjointed and ineffective. Industry lobbyists including the Australian Bankers Association claim there has been little progress in co-ordinating the fight against cybercrime over the past five years because of poor government leadership that has left internet-dependent industries sitting on the sidelines….
>
> After demonstrating for the ABC's Four Corners program on Monday night how police covertly take control of websites used to sell fraud software, the AFP later conceded the criminals they targeted had hacked back into the police computer used to seize the website, prompting a major security scare. State police also have problems with their federal peers. A submission to the cybercrime inquiry from the South Australia Police claims "national multi-agency initiatives are rarely developed and implemented".[44]

Sobering commentary indeed on the current e-security policy arrangements found here. We all face the problems of increasing crime and insecurity online, whether we like it or not:

> Despite all the publicity about cybercrime, low levels of security on home computers, insecure wireless networks, theft and loss of hardware and plain gullibility mean that criminal networks are likely to continue to find cybercrime immensely profitable. As the Federal Police point out, "Home [internet users] are particularly vulnerable to intrusion and online banking fraud due to lower levels of computer security awareness and education, and the presence of unprotected sensitive personal information (such as financial details) on their machines. The machines of the novice home user present a particularly easy target for recruitment into botnets – and compromised machines continue to be used for attacks against commercial and government networks."
>
> In the new world of high-speed broadband, there is an ever-closer convergence between the personal and home security of individuals and the security of major financial institutions and processes, and indeed of government. Interconnectedness cuts all ways … At the very least,

44. J Bajkowski, 'Cybercrime inquiry, warnings unheeded', *Australian Financial Review*, 20 August 2009, p. 58, http://parlinfo.aph.gov.au/parlInfo/download/media/pressclp/X0GU6/upload_binary/x0gu60.pdf;fileType=application/pdf#search=%22cybercrime%20inquiry%22.

> there is a strong case for the Australian Government not only to invest heavily in improving the security of its own networks, but also in wide-ranging security education and public awareness campaigns to support the home security of millions of Australians who are ever-more-reliant on the internet to conduct their everyday lives. [45]

Australian Cyber Security Policy

The Australian Government approach to e-security was established by the E-Security National Agenda (ESNA) in 2001 and reviewed in 2006. In July 2008 a comprehensive E-Security Review of the Australian Government's e-security arrangements was conducted by a multi-agency team. A key outcome of the Review was to be a new policy framework for e-security, covering the span of e-security issues across government, business and the community. The new framework would articulate the Australian Government's e-security objectives and identify the strategies and capabilities required to achieve the aim of maintaining a secure and trusted electronic operating environment for both the public and private sectors.[46] This framework would become the new 2009 Cyber Security Strategy.

In December 2008, the Prime Minister responded to an earlier review of homeland and border security and ICT. For reasons of national security, the report was not made public, but the Summary and Conclusions of the Review were published on 4 December 2008:

> Electronic attack is a significant new means of compromising national security and enabling criminal activity. Governments, businesses and individuals are increasingly vulnerable to such attacks. The Commonwealth has a special role to play in this area given its high level capabilities in e-security and the cross-jurisdictional nature of the threat. It is however difficult to quantify the magnitude of the problem and the potential economic and social consequences, particularly of a large-scale cyber attack. An independent risk analysis of the e-security environment should be commissioned to better inform the strategic direction of our efforts. Current arrangements within the Australian Government for ensuring effective e-security generally work well, although it is an area in need of consistent senior policy attention. In some areas roles and responsibilities should be clarified to avoid confusion and possible duplication of effort. These issues should be addressed as part of the current e-security review being led by the Attorney-General's Department, which has the lead role in this area.

In May 2009, the Commonwealth Attorney-General, the Hon Robert McClelland announced new e-security arrangements:

---

45. P Dorling, 'Netted on the web', *The Canberra Times* 22 August 2009, pp. Forum 1–4, http://parlinfo.aph.gov.au/parlInfo/download/media/pressclp/UYGU6/upload_binary/uygu64.pdf;fileType=application%2Fpdf#search=%22netted%20on%20the%20web%22.

46. Attorney-General's Department Submission to the House of Representatives, Standing Committee on Communications, Inquiry into Cyber Crime, July 2009, viewed 15 September 2009, http://www.aph.gov.au/house/committee/coms/cybercrime/subs/sub44.pdf.

> Recognising the Australian community's increasing reliance on information and communications technology in all aspects of life, the Commonwealth will provide $8.8 million on e-security, to bring together Australia's existing computer emergency response arrangements under a new national Computer Emergency Response Team (CERT). The new national CERT, to be created in collaboration with AusCERT, will provide a single point of contact for e-security information for all Australians and Australian businesses. It will also ensure Australian internet users have access to information on cyber threats, vulnerabilities in their systems and information on how to better protect their information technology environment. [47]

Cyber Security Strategy

On 23 November 2009, the Attorney-General, the Hon Robert McClelland MP launched the Cyber Security Strategy, CERT Australia and Identity Theft Booklet.[48] He stated that:

> The new Australian Government Cyber Security Strategy describes the way in which the Government is tackling security threats to our computers. And it has three main goals that reflect the three elements of individuals, business and government. The first goal is for all Australians to know about online security threats, to know how to secure their computers, and to know how to help protect their identities, privacy and finances online. The second goal is for all Australian businesses to operate secure and resilient computer systems to protect their operations, and the identity and privacy of their customers. And the third goal is for the Australian Government to make sure our computer systems are secure and resilient, particularly as we are the custodians of information on taxpayers and citizens. To achieve these goals the Australian Government is going to give all Australians the information, confidence and practical tools needed to be secure online. We're also going to work with business and our international partners to help create a culture of security on the Internet.
>
> Today I would like to announce the name of the new Australian Government national CERT (Computer Emergency Response Team). It is called CERT Australia. It brings together our national computer emergency response team arrangements. And it will be the national coordination point for providing cyber security information and advice to all Australians.

---

47. Attorney-General, *Strengthening our National Security*, Media Release, 12 May 2009, viewed 15 September 2009, http://www.ag.gov.au/www/agd/agd.nsf/Page/Publications_Budgets_Budget2009_MediaReleases_StrengtheningOurNationalSecurity.

48. Australian Government, *Cyber Security Strategy*, Attorney General's Department, Canberra 2009, viewed 18 December 2009, http://www.ag.gov.au/www/agd/rwpattach.nsf/VAP/(4CA02151F94FFB778ADAEC2E6EA8653D)~AG+Cyber+Security+Strategy+-+for+website.pdf/$file/AG+Cyber+Security+Strategy+-+for+website.pdf/, Attorney-General for Australia, 'Launch of the Cyber Security Strategy, Cert Australia and Identity Theft Booklet', *Speeches by the Hon Robert McClelland MP*, 23 November 2009, viewed 18 December 2009, http://www.attorneygeneral.gov.au/www/ministers/mcclelland.nsf/Page/Speeches_2009_FourthQuarter_23November2009-LaunchoftheCyberSecurityStrategy,CertAustraliaandIdentityTheftBooklet.

> CERT Australia will also be the initial point of contact for international agencies to let Australia know about cyber security issues. It will work with other national CERTs around the world, the IT industry and Australian Internet Service Providers to help network operators identify and respond to cyber security incidents.
>
> The new CERT Australia will continue to build on the work of the Australian Government Computer Emergency Readiness Team, or GovCERT.au – currently helping owners and operators of critical infrastructure secure their networks and systems. CERT Australia will begin initial operations in January and will be fully operational by July next year. It will be managed by my Department and will work closely with the Cyber Security Operations Centre (CSOC). The CSOC has been established following the Defence White Paper released in May this year.
>
> I am also very pleased today to launch the new Identity Theft Booklet – *Protecting your Identity*. It provides Australians with practical advice and strategies on how to protect personal and financial information, as well as information on our computers and what to do if we've been a victim of identity theft. The booklet also includes a checklist to assess how vulnerable we are to identity crime and provides a list of government resources to help protect our personal information.[49]

The Attorney-General's Department website on Cyber Security outlines national policy:

> **Cyber Security**
>
> The Attorney-General's Department is the lead agency for cyber security policy across the Australian Government and chairs the Cyber Security Policy and Coordination (CSPC) Committee, which is the interdepartmental committee that coordinates the development of cyber security policy for the Australian Government. The Australian Government's cyber security policy is contained in its Cyber Security Strategy.
>
> The Strategy was launched on 23 November 2009 and articulates the overall aim and objectives of the Australian Government's cyber security policy and sets out the strategic priorities that the Australian Government will pursue to achieve these objectives. The Strategy also describes the key actions and measures that will be undertaken through a comprehensive body of work across the Australian Government to achieve these strategic priorities.
>
> The Strategy was a key outcome of the E-Security Review 2008[50] The Review examined the Australian Government's cyber security policy, programs and capabilities with the aim of developing a new Australian Government policy framework for cyber security – the Strategy. The Australian Government defines cyber security as: *Measures relating to the*

49. Ibid.

50. Attorney-General's Department E-Security Review website, viewed 20 February 2010, http://www.ag.gov.au/www/agd/agd.nsf/Page/Consultationsreformsandreviews_E-SecurityReview_E-SecurityReview.

> *confidentially, availability and integrity of information that is processed, stored and communicated by electronic or similar means.*
>
> The aim of the Australian Government's cyber security policy is: *The maintenance of a secure, resilient and trusted electronic operating environment that supports Australia's national security and maximises the benefits of the digital economy.*[51]

Cyber Security Program Agencies

The Attorney-General's Department submission to the cyber crime Inquiry briefly outlines the current administrative arrangements, and they are also summarised on the department's website, as described in the following fifteen paragraphs.[52] The Australian Government's e-security programs are delivered by a number of Australian Government agencies, including:

The **Attorney-General's Department (AGD)** is responsible for developing Australian Government protective security policy and criminal justice. It is the lead policy agency for e-security and takes a lead role in advancing business-government partnerships and providing e-security guidance to owners and operation of critical infrastructure and other systems of national interest. It also has responsibility for criminal law and law enforcement including administration of the Criminal Code. AGD takes a leadership role in advancing business-government partnerships, including national CERT arrangements, and provides cyber security guidance to owners and operators of critical infrastructure and other businesses of national interest. CERT Australia works with the Joint Operating Arrangements (JOA) agencies to contribute to a shared understanding of major events, provide a pathway to the national crisis management arrangements, to provide alerts and guidance to the private sector.

The **Australian Communications and Media Authority (ACMA)** is responsible for regulation of broadcasting, the Internet, radio-communications and telecommunications. As part of its role, it gathers evidence and assists in protecting Australians from computer fraud and identity theft. ACMA ensures internet service providers (ISPs) and telecommunications providers are meeting their regulatory obligations regarding criminal misuse and illegal content by encouraging the development of codes of practice for ISPs and online content service providers and monitoring compliance with these codes. It identifies, investigates and acts against those involved in the distribution of spam.

---

51. Attorney-General's Department website, viewed 19 February 2010, http://www.ag.gov.au/www/agd/agd.nsf/Page/CyberSecurity_CyberSecurity.

52. Attorney-General's Department, *Submission to the House of Representatives Standing Committee on Communications Inquiry into Cyber Crime*, July 2009, viewed 19 February 2010, http://www.aph.gov.au/house/committee/coms/cybercrime/subs/sub44.pdf. Attorney-General's Department Cyber Security website, viewed 20 February 2010, http://www.ag.gov.au/www/agd/agd.nsf/Page/CyberSecurity_CyberSecurity.

The **Australian Federal Police (AFP)** enforces Commonwealth criminal law and protects Commonwealth and national interests from crime in Australia and overseas. It provides a specialised investigative capacity to support the identification and investigation of complex technology enabled crime offences, in partnership with the Australian law enforcement community. It actively engages in the implementation of crime prevention strategies aimed at raising awareness of cyber security risks in the Australian community The AFP also collaborates with international agencies to address technology enabled crime issues. The AFP is a member agency of the JOA.

The Department of Finance and Deregulation's **Australian Government Information Management Office (AGIMO)** works with Australian Government agencies to ensure the productive application of ICT. It contributes to cyber security objectives by ensuring that Australian Government ICT proposals have adequately considered cyber security risks. AGIMO works with agencies to adopt a whole of government approach to the management of common assets and data sharing, to promote security and resilience. It develops whole of government strategies to help meet shortfalls in skilled cyber security practitioners, and coordinates a strategy for managed internet gateways for Australian Government agencies.

The **Australian Security Intelligence Organisation (ASIO)**'s responsibilities include investigating electronic attacks conducted for purpose of espionage, sabotage, terrorism, or other forms of politically motivated violence, attacks on the defence system and other matters that fall under the heads of security. ASIO collects intelligence both domestically and internationally on such matters, assessing the capabilities and intentions of persons and groups of security interest. ASIO contributes to the investigation of computer network operations directed against Australia's national interests, including those targeting government and critical infrastructure assets. ASIO produces threat assessments and protective security advice for government and critical infrastructure, and liaises with business on behalf of the Australian intelligence community through the Business Liaison Unit.

The **Defence Signals Directorate (DSD)** is the national authority on the security of ICT across government including threats posed to government ICT by cyber crime. DSD provides a range of information security services to ensure that sensitive government electronic information systems are not susceptible to unauthorised access, compromise or disruption. DSD provides material, advice and other assistance to Commonwealth and State authorities on matters relating to the security and integrity of information that is processed, stored or communicated by electronic or similar means. DSD provides assistance to Commonwealth, State and Territory authorities in relation to cryptography and communications technologies. DSD, through the CSOC, is responsible for maintaining a comprehensive national picture of cyber security threats, through monitoring and analysis of all information sources. It provides a central point for sharing information across government and coordinates with other agencies on response activities. DSD is responsible for developing and maintaining the Australian Government Information and Communications Technology Security Manual (ISM). It is a member agency of the JOA.

The **Department of Broadband, Communications and the Digital Economy (DBCDE)** is responsible for creating an environment that allows Australians to take full advantage of the opportunities offered by the digital economy. It works with industry and the community to raise awareness of e-security risks, including the risk of cyber crime, with a view to improving their online practices and behaviours. [53]

As well, the **Australian Institute of Criminology (AIC)** has undertaken research into various forms of crime utilizing electronic communications and computing systems. Among numerous papers, the AIC's major works have been publications on crime in the digital age and electronic theft: crimes of acquisition in cyber space, as monographs on the risks associated with conducting business and other forms of communication in cyber space.[54]

AusCERT is the national Computer Emergency Response Team (CERT) for Australia and a major CERT in the Asia-Pacific region. It is the primary Australian contact for dealing with Internet security threats and vulnerabilities affecting our interests. It operates within a world-wide network of information security experts and provides computer incident prevention, response and mitigation strategies for members and assistance to affected parties here.[55]

A new **Cyber Security Operations Centre (CSOC)** is to provide the Australian Government with cyber situational awareness, coordinate responses to e-security incidents of national importance and will maintain a 24x7 watch on cyber activities which might threaten Australia's national security. The Department of Defence's submission to the Cyber Crime Inquiry clarifies this:

> A Cyber Security Operations Centre will become the new frontline under the White Paper initiative to provide better situational awareness and the ability to facilitate responses to cyber security incidents. The new Cyber Security Operations Centre will be staffed by skilled experts to maximise the Government's ability to detect and rapidly respond to fast-evolving and aggressive cyber attacks. It will do this by drawing on an array of sources in the intelligence, law enforcement and industry communities to provide a comprehensive picture of threats to Australian information and systems. It will also act as a coordination point for responses by Government agencies and will work in close collaboration with overseas partners. [56]

---

53. Attorney-General's Department Submission to the House of Representatives, Standing Committee on Communications, Inquiry into Cyber Crime, July 2009, viewed 15 September 2009, http://www.aph.gov.au/house/committee/coms/cybercrime/subs/sub44.pdf.

54. Australian Institute of Criminology cybercrime website, viewed 7 October 2009, http://www.aic.gov.au/crime_types/cybercrime.aspx.

55. AusCERT website, viewed 15 September 2009, http://www.auscert.org.au/.

56. Department of Defence Submission to the House of Representatives, Standing Committee on Communications, Inquiry into Cyber Crime, July 2009, viewed 15 September 2009, http://www.aph.gov.au/house/committee/coms/cybercrime/subs/sub20.pdf.

The **Australian Government's Critical Infrastructure Protection (CIP)** operates through the Trusted Information Sharing Network (TISN) for Critical Infrastructure Protection.[57] The TISN, which is led by the Attorney-General's Department, is a forum in which the owners and operators of critical infrastructure work together with the Government to share information on security issues that affect critical infrastructure. The Australian Government Computer Emergency Readiness Team (GovCERT.au) assists e-security policy formulation for national computer emergency preparedness, response, readiness and recovery.[58]

The **Joint Operating Arrangements** (JOA) were established by the Australian Government whereby operational cyber security agencies (DSD, AFP and ASIO) to identify, analyse and respond to cyber events of serious national consequence. The JOA agencies determine which agency has primary carriage of a security event response on the basis of the nature of the event and individual agency responsibilities.

The **Cyber Security Policy and Coordination (CSPC) Committee** is the Australian Government interdepartmental committee that coordinates the development of cyber security policy for the Australian Government. The CSPC Committee provides whole of government strategic leadership on cyber security. It determines priorities for the Australian Government and coordinates the response to cyber security events, noting that its coordination and policy functions do not extend to the oversight of operations.

The **Internet Industry Association (IIA)** has released a draft e-security code to guide ISPs in improving net security for its users throughout Australia.[59] The draft Code has four main elements of identifying compromised computers; customer contact; provision of information and advice to fix the compromised system and a reporting function for alerting about serious scale threats, such as those, that may threaten national security.

National Security Science and Innovation Strategy

On 4 December 2008, the Prime Minister called for national security standards for online activity and that, in response, in November 2009, the National Security Science and Innovation Strategy was released by the Department of Prime Minister and Cabinet.[60] This

57. Trusted Information Sharing Network website, viewed 15 September 2009, http://www.tisn.gov.au/.

58. GovCERT.au website, viewed 15 September 2009, http://www.ag.gov.au/govcert.

59. J Hilvert, *eSecurity Code to protect Australians online* (draft), Internet Industry Association, 11 September 2009, viewed 15 September 2009, http://www.iia.net.au/index.php/section-blog/90-esecurity-code-for-isps/757-esecurity-code-to-protect-australians-online.html.

60. Prime Minister, The First National Security Statement, to the Parliament, Address by the Prime Minister of Australia, The Hon. Kevin Rudd MP, 4 December 2008, viewed 20 February 2010, http://www.pm.gov.au/node/5424. Department of the Prime Minister and Cabinet, National Security Science and Innovation Strategy website, viewed 20 February 2010, http://www.dpmc.gov.au/nsst/strategy.cfm.

strategy established a set of twelve national security objectives for science and innovation and an annual process for the national security community to communicate their science and innovation priorities to researchers, entrepreneurs and funding programs. The objectives include matters of cyber protection, resilience, information management, surveillance, policy standards and response. An example is Critical Infrastructure Protection Modelling and Analysis (CIPMA) where government agencies have developed a capability to model the complex inter-dependencies between critical infrastructure systems, and how a failure in one sector can greatly affect the operations of other sectors such as banking and finance, communications, and energy. The Strategy says that a number of research agencies undertake science and innovation for national security:

 The **Australian Institute of Criminology (AIC)** provides analysis of complex and sophisticated criminal activity, including economic crime, high-tech and cyber crime, transnational and organised crime, money laundering and crimes against the environment and natural resources.

 The **Australian Nuclear Science and Technology Organisation (ANSTO)** supports national security through its nationally unique capability to deliver nuclear scientific and technological research for both nuclear-related requirements and enhancements to screening and detection technologies.

 The **Commonwealth Scientific and Industrial Research Organisation (CSIRO)** already addresses a range of traditional and new national security areas in its research, including in animal and plant biosecurity, sensor networks and automated biological and chemical detectors, intelligent information and communication technology, and disease spread forecasting.

 The **Defence Science and Technology Organisation (DSTO)** supports civilian national security requirements through leveraging defence-related research and development capabilities, including in chemical, biological and nuclear defence; explosives effects and improvised explosive devices; intelligence-related technologies; and cyber security.

 Geoscience Australia (GA) contributes to the Critical Infrastructure Protection Modelling and Analysis program managed by the Attorney-General's Department, while its broader program of work on earth monitoring, natural hazards, energy security and geospatial data has a growing role to play in enabling our responses to new and emerging threats to national security.

 National Information and Communications Technology Australia (NICTA) contributes to national security research in areas such as the enhancement of intelligent CCTV systems and evaluation and enhancement of current wireless mesh technologies to assist emergency services.

 The **National Measurement Institute (NMI)** delivers essential services that have national security relevance, including chemical and biological analysis, pattern approval testing and supporting to Australia's standards and conformance infrastructure.[61]

Overseas Cyberspace Security Strategy

United States

In 2003, the Bush Administration announced "The National Strategy to Cyberspace Security" as the security blueprint for the United States.[62] The document continued work commenced by the Department of Homeland Security for improving the country's cyber security. The document's scope covered all government sectors, private sectors and the American people. It proposed five major goals of: building a national cyberspace security response system; develop a treat and vulnerability reduction system; expanding awareness and training programs; securing the government's cyberspace; and promoting national security and international cyberspace community cooperation.

According to the 2008 U.S. Congressional Research Service Report to Congress on *Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress*:

> Cybercrime is becoming more organized and established as a transnational business. High technology online skills are now available for rent to a variety of customers, possibly including nation states, or individuals and groups that could secretly represent terrorist groups. The increased use of automated attack tools by cybercriminals has overwhelmed some current methodologies used for tracking Internet cyberattacks, and vulnerabilities of the U.S. critical infrastructure, which are acknowledged openly in publications, could possibly attract cyberattacks to extort money, or damage the U.S. economy to affect national security.[63]

The Australian Institute of Criminology submission to the cyber crime inquiry here provides an overview of the more recent (Obama) U.S. policy changes to cyber security policy:

> A 2008 report of the Center for Strategic and International Studies (CSIS) Commission on Cybersecurity for the 44th Presidency noted: 'we began with one central finding: The United States must treat cybersecurity as one of most important national security challenges it faces' (CSIS 2008). A National Office for Cyberspace will be established within the

61. Department of the Prime Minister and Cabinet, *The National Security Science and Innovation Statement*, Department of the Prime Minister and Cabinet, Canberra 2009, viewed 18 December 2009, http://www.dpmc.gov.au/nsst/docs/NSSIS_strategy.pdf.

62. Department of Homeland Security website, viewed 20 February 2010, http://www.dhs.gov/files/publications/editorial_0329.shtm.

63. Congressional Research Service, 'Botnets, cybercrime, and cyberterrorism: Vulnerabilities and policy issues for Congress', *CRS Report to Congress*, Washington, 28 January 2008, viewed 7 October 2008, http://fas.org/sgp/crs/terror/RL32114.pdf.

> Executive Office of the President under the United States Information and Communications Enhancement Act of 2009 to deal with the emerging cybersecurity threats. The office is tasked to coordinate cybersecurity response between the Department of Homeland Security, the Department of Defense, the National Security Agency and the private sector. On 29 May 2009, the President of the United States of America Barack Obama referred to the importance of cyber threats faced in today's digital age.[64]

For convenience here, the draft report of the Australian Government 2.0 Taskforce provides some insight into the US changes:

> The day after his inauguration in January this year, President Obama issued two memoranda to agency heads which clearly set out his intentions for government to be accountable, transparent, participatory and collaborative. This followed the well-publicised use of information technology to engage with the public during his election campaign.[65]

In May 2009, President Obama announced special measures on *Securing Our Nations Cyber Infrastructure* by revealing that he and the nation had been subject to e-security failures.[66] The plans aim to shore up the safety of U.S. computer networks, including naming a new 'Cybersecurity Coordinator'. Implementation of U.S. national ICT security programs previously occurred under the Department of Homeland Security and other defence agencies.

In February 2009 the Obama Administration commissioned Melissa Hathaway to conduct a 60-day review of US cyber security policies and structures. The *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure* was presented in May 2009.[67] This Cyberspace Policy Review to the President contained five main chapters, and included a near-term ten step action plan for U.S. Government activities to strengthen cyber security.

There are host of other American organisations concerned with fighting cyber crime. This section has just touched on the overall thrust of current overarching U.S. policy direction.

---

64. Australian Institute of Criminology, Submission to the House of Representatives, Standing Committee on Communications, Inquiry into Cyber Crime, July 2009, viewed 20 February 2010, http://www.aph.gov.au/house/committee/coms/cybercrime/subs/sub41.pdf.

65. Government 2.0 Taskforce, *Engage: Getting on with Government 2.0*, Australian Government Information Management Office, Department of Finance and Deregulation, viewed 19 February 2010, http://www.finance.gov.au/publications/gov20taskforcereport/index.html.

66. The White House, Office of the Press Secretary, *Remarks by the President*, 29 May 2009, viewed 15 September 2009, http://www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure/.

67. The White House, *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure*, viewed 15 September 2009, http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf.

United Kingdom

According to the ASPI *Special Report*, MacGibbon notes that:

> In June 2009 UK Prime Minister Gordon Brown delivered the UK's first Cyber Security Strategy. The strategy concluded with the following assessment:
>
> > Just as in the nineteenth century we had to secure the seas for our national safety and prosperity, and in the twentieth century we had to secure the air, in the twenty first century we also have to secure our position in cyber space in order to give people and businesses the confidence they need to operate safely there.[4]
>
> The strategy argues that economic considerations alone make cyber security a priority: 90 percent of offline purchases use credit or debit cards relying upon telecommunications systems; £50 billion in e-commerce transactions occur each year. As part of the strategy, the British Government has established an Office of Cyber Security and appointed a Cyber Security Minister.
>
> UK government capabilities and policy developments have more in common with Australia than the US experience. In fact, the UK program of work is almost identical to that in Australia's Attorney–General's Department. A significant point of departure between the British and Australian responses has been the notion of privacy which receives less attention in current Australian thinking.
>
> It is also of note that in May 2009 Australia—and in June 2009 the US and the UK—announced the formation of operational cyber defence centres within their respective signals intelligence agencies: the Cyber Security Operations Centre as part of the Defence Signals Directorate (DSD) in Australia, Government Communications Headquarters in the UK, and the Cyber Command within the US National Security Agency.[68]

The 2009 *Digital Britain: the final report* does not comment on the risks posed by cyber crime activities even though it includes a section on digital security and safety.[69] An October 2006 *postnote* on computer crime from the UK Parliamentary Office of Science and Technology says:

> The increasing range of programmable electronic devices, from set-top TV boxes to mobile phones, means that 'computer' crime can affect more than just personal computers (PCs).

68. A MacGibbon, 'Cyber security: Threats and responses in the information age', Australian Strategic Policy Institute, *Special Report*, Issue 25, Canberra, December 2009.

69. Department for Business, Innovation and Skills, *Digital Britain: The Final Report*, May 2009, viewed 15 September 2009, http://digitalbritainforum.org.uk/report/category/executive-summary/.

> They and other electronic devices are particularly vulnerable to attack because they are flexible, can be reprogrammed, and are frequently networked with other devices. [70]

Nowadays, the Centre for Protection of National Infrastructure (CPNI) is the Government authority that provides protective security advice to businesses and organizations across the national infrastructure.[71] In regards to computer crime, the CPNI notes that:

> **Electronic attacks**
>
> The potential for electronic attack against your computer networks is enormous. As users demand software with more features and services to improve business delivery, new opportunities for exploitation will continue to emerge.
>
> CPNI examines all types of electronic attack on information and process control systems that form part of the UK's critical national infrastructure. This could include malware, hacking, botnets, keystroke logging, phishing and denial of service. We liaise with vendors about the responsible disclosure of patches for vulnerabilities discovered in their products, helping to prevent attacks that use previously unpublished vulnerabilities.
>
> We recommend that all systems are patched and have current, up-to-date, anti-virus software and a firewall that restricts access on to services that users need for their business (typically web and email).
>
> The UK statistics on network growth and speeds are dramatic. Broadband access is predominantly by Asynchronous Digital Subscriber Line (ADSL) connections and these are getting faster and more widespread. Wireless connectivity is also growing rapidly; a key implication of this unprecedented wireless connectivity is that attackers can reach you at all times.
>
> Threats always evolve. The convergence of networking and telecommunications technologies around the Internet Protocol (IP) will likely lead to vulnerabilities being discovered in any new technologies, for example telecommunications networks rely on IP. Generally, vendors are improving the security of their products, including timely patch provision, so we expect to see new types of software applications being targeted - such as back-up software - which is a trend supported by the latest SANS Top 20, see SANS Top 20 website.[72]

---

70. Parliamentary Office of Science and Technology (POST), 'Computer crime', *postnote*, no. 271, October 2006, viewed 15 September 2009, http://www.parliament.uk/documents/upload/postpn271.pdf.

71. Centre for the Protection of National Infrastructure, website viewed 15 September 2009, http://www.cpni.gov.uk/.

72. SANS Top Cyber Security Risks website, viewed 20 February 2010, http://www.sans.org/top-cyber-security-risks/?ref=top20#_blank.

Linked to CPNI the UK Warning, Advice and Reporting Point (WARP) community website provides an up-to-date self-help service to counter crime.

Europe and the International Strategy Framework

orty-three countries, have signed the Council of Europe's Convention on Cybercrime of November 2001.[74] The Convention seeks to better combat cyber crime by harmonizing national laws, improving investigative abilities, and boosting international cooperation.[75] According to one study, supporters argue that the Convention will enhance deterrence while critics counter it will have little effect without participation by countries in which cyber criminals operate freely. Others warn it will endanger privacy and civil liberties.[76]

> In the Council of Europe's *Cybercrime Treaty* (EST no. 185), cybercrime is used as an umbrella term to refer to an array of criminal activity including offences against computer data and systems, computer-related offences, content offences, and copyright offences. This wide definition of cybercrime overlaps in part with general offence categories that need not be ICT dependent.

In early 2009, IMPACT (the International Multilateral Partnership against Cyber Threats) set up a Global Response Centre (GRC) in Malaysia, as a cyber-threat resource, to proactively track and defend against cyber-threats. The centre's alert and response capabilities including an Early Warning System that enables IMPACT members to identify and head-off potential and imminent attacks before they can inflict damage on national networks.

On 6 October 2009, the United Nations International Telecommunications Union Secretary-General said that the next world war could take place in cyber space. He said that countries needed to be aware that there was no such thing as a superpower in a cyber war and loss of vital networks would quickly cripple any nation. His warning came as experts called for action to stamp out cyber attacks, as current software and web infrastructure has the same weaknesses as those produced two decades ago.[77] It seems that little has changed except the risk of the threat and its consequences.

---

73. Warning, Advice and Reporting Point website, viewed 15 September 2009, http://www.warp.gov.uk/.

74. Council of Europe website, Convention on Cybercrime Budapest, 23.XI.2001, viewed 20 February 2010, http://conventions.coe.int/Treaty/EN/Treaties/html/185.htm.

75. Note that Australia has signed but is not a party to the CoE.

76. Congressional Research Service, 'Cybercrime: The Council of Europe Convention', *CRS Report to Congress*, Washington, 28 September 2006, viewed 7 October 2009, http://www.au.af.mil/au/awc/awcgate/crs/rs21208.pdf.

77. Hui Min Neo, 'Cyberspace `world war' catastrophic: UN warns', *The Canberra Times*, 8 October 2009, viewed 8 October 2009, http://parlinfo.aph.gov.au/parlInfo/download/media/pressclp/SFVU6/upload_binary/sfvu60.pdf;

Policy Outlook

The ASPI Cyber Security Report provides some useful findings that bear repetition here.[78] The author MacGibbon believes that e-security is a shared responsibility but faces issues of scale, timeliness, jurisdictional boundaries, identification aspects and policy linkages MacGibbon concludes that the 'light touch' policy had failed and that the Defence Signals Directorate has to tighten security requirements of Australian Government data and systems. He also believes that the Commonwealth has to impose security requirements on industry in areas such as lost data handling and privacy controls. Public and business education was a big task but needs to improve, for example, in the manner of public health programs.

Jurisdictional problems and cyber crime fighting capacity needed clarification. MacGibbon says that the Government should require Internet Service Providers to act to protect users in a manner akin to the role of banks in protecting our accounts and personal details. While there is no international quantified estimate of the security threat it is there nonetheless, he believes. So he expects more action from governments, be it through special initiatives, although any counter attacks, as such, would be best left to the Australian Defence Force.

Regarding defence agencies, among specific recommendations, the Gov 2.0 reports states that:

> **Recommendation 8 – Security and Web 2.0**
>
> The Defence Signals Directorate (DSD) should provide guidance to agencies on the appropriate mitigation treatments that could be adopted to address concerns or exposures identified in relation to the use of social networking and related tools. This guidance is to take into consideration the different environments that agencies operate in, the varying risk profiles that exist and the range of tools that may be used. DSD should update the Information Security Manual (ISM) accordingly.
>
> The lead agency, in conjunction with DSD, should develop a Better Practice Guide (or "how to guide") to assist agencies in the effective, efficient and secure use of Web 2.0 tools and how to undertake associated risk assessment.
>
> Sensitive and National Security data requires special consideration in the context of PSI. To ensure consistency between PSI arrangements in the future and the proposed changes to the FOI Act, the proposed new Office of the Information Commissioner should provide advice to agencies in relation to the treatment of PSI to enable its broadest possible release. Consistent with good practice, and the requirements of the Protective Security Manual

---

fileType=application/pdf#search=%22united%20nations%22 and http://www.itu.int/newsroom/press_releases/2009/40.html.

78. A MacGibbon, ASPI, op. cit.

> (PSM), agencies must avoid the over classification of data so as to limit the need to review or pre-process data to enable its release.[79]

The Gov2.0 Taskforce draft report notes the existence of the Information Security Manual:

> The basis of information technology security in the Australian Government is described in the Information Security Manual (ISM) (PDF), published by the Defence Signals Directorate (DSD). This document, updated regularly, provides a broad set of recommendations for maintaining IT security in government agencies. The recommendations are based on a set of principles covering all aspects of IT security. Compliance with all aspects of the ISM is mandated for Commonwealth agencies unless a specific waiver is granted. Following are some relevant extracts from the current edition of the PSM:…***Accessing social networking websites:*** *4.1.90. It is recommended that agencies prevent personnel from accessing social networking websites that pose a higher than normal security risk relating to the unauthorised release of government information or disclosure of personal information. 4.1.100. Websites that may pose a higher than normal security risk relating to the unauthorised release of government information or disclosure of personal information can include, but are not limited to, websites such as Facebook, Myspace and Twitter.*[80]

Clearly though, our policies must recognise events occurring overseas, given the global and instant nature of the Internet. Other issues mentioned in the Attorney-General's submission to the cyber crime inquiry include cyber terrorism, identity management, telecommunications interception, privacy, consumer fraud and cyber safety. All of these themes have been taken up by governments, but have not been covered in this summary document.

According to James Riley in Exchange weekly, commenting on the Gov2.0 draft report, a roadmap is still needed:

> But within the motherhood statements and idealism of its recommendations, the 129-page draft report highlights the gulf between the apparent expectations of the 2.0 community and some core realities of public administration. The draft highlights the benefits of improved online engagement but has not yet provided a realistic roadmap to achieve those outcomes.[81]

---

79. Government 2.0 Taskforce, *Engage: Getting on with Government 2.0*, Australian Government Information Management Office, Department of Finance and Deregulation, viewed 19 February 2010, http://www.finance.gov.au/publications/gov20taskforcereport/index.html.

80. Ibid, Chapter 11: Other Issues and Challenges, 11.1: Government 2.0 and Security. viewed 19 February 2010, http://www.finance.gov.au/publications/gov20taskforcereport/index.html. Defence Signals Directorate website, Australian Government Information Security Manual, September 2009, viewed 20 February 2010, http://www.dsd.gov.au/_lib/pdf_doc/ism/ISM_Sep09_rev1.pdf.

81. J Riley, 'Government 2.0 draft report: a blueprint for cultural change', *Exchange,* 11 December 2009, Vol–21 No. 47.

There would then seem to be more work needing to be done to assuage the twitter risk.

Acknowledgements

This brief benefited from comments made by Ann Rann, Joanne James, Peter Hicks, Monica Biddington and Roger Beckman, who are gratefully acknowledged. Special thanks are due to Dr Lawrie Brown from the ADFA School of Engineering and Information Technology for his comments.

© Copyright Commonwealth of Australia

This work is copyright. Except to the extent of uses permitted by the *Copyright Act 1968*, no person may reproduce or transmit any part of this work by any process without the prior written consent of the Parliamentary Librarian. This requirement does not apply to members of the Parliament of Australia acting in the course of their official duties.

This work has been prepared to support the work of the Australian Parliament using information available at the time of production. The views expressed do not reflect an official position of the Parliamentary Library, nor do they constitute professional legal opinion.

Feedback is welcome and may be provided to: web.library@aph.gov.au. Any concerns or complaints should be directed to the Parliamentary Librarian. Parliamentary Library staff are available to discuss the contents of publications with Senators and Members and their staff. To access this service, clients may contact the author or the Library's Central Entry Point for referral.