INDO-PACIFIC STRATEGIC PAPERS

Cyber Security: Time for an integrated whole-of-nation approach in Australia

Chris Brookes

MARCH 2015

VICE CHIEF OF THE DEFENCE FORCE
Australian Defence College
Centre for Defence and Strategic Studies

The Centre for Defence and Strategic Studies (CDSS)

CDSS is the senior educational institution of the Australian Defence College. It delivers a one-year Defence and Strategic Studies Course, a professional development program that places emphasis on practical rather than theoretical research, on teamwork and support for the personal and professional goals of students. Students and staff share a commitment to achieving professional excellence. Students graduate with a range of postgraduate qualifications in strategic studies, policy and politics, and business administration.

In addition, CDSS is home to the Centre for Defence Leadership and Ethics (CDLE) and the Centre for Defence Research (CDR). CDR manages the publications on behalf of CDSS staff and students.

Indo-Pacific Strategic Papers

This range of papers reflects coursework and research submitted by Australian and international students of the Defence and Strategic Studies Course, as well as staff. The papers have been chosen for publication based on their scholarly attributes and strategic relevance. The topics of the papers relate to Australia's area of primary and enduring strategic interest—the Indo-Pacific region—and present analyses and assessments that concern Australia's policy interests.

For further information about CDSS publications, please visit
<http://www.defence.gov.au/adc/publications/publications.html>

Copyright

Disclaimer

The author

Chris Brookes is an Executive Level 2 APS in the Department of Defence. He graduated from ANU in 2002 with a double degree in Economics and Information Technology. He has since held a number of roles in both industry and government, primarily in the cyber and information security field, including with Deloitte, the Australian Bureau of Statistics, CRS Australia and Verizon Business.

In 2010, Chris took up a role within Defence in the cyber security field, providing ICT security advice, assistance and expertise to Defence and the broader Australian Government. In January 2013, Chris was seconded to the Chief Information Officer Group in Defence to undertake a review and reform of ICT security in Defence. He attended the Defence and Strategic Studies Course at CDSS at the Australian Defence College in 2014, and is currently again working in cyber security in the Department of Defence.

Abstract

While terrorism and specifically the Islamic State are dominating the national security agenda at the moment, this paper contends that cyber security is still an important issue for the Australian Government. The issue can be articulated both in terms of the economic costs and personal impacts that cyber threats have on businesses and individuals in Australia, as well as the potential impacts, given current reliance on online social and financial interactions, should Australians lose confidence in the security of online interactions because of cyber threats.

The paper acknowledges that it is impossible for the Australian Government to directly provide cyber security capabilities for the entire business and civilian population. However, it asserts that the direct costs, the potential future impact, and the second-order effects of cyber threats require the Australian Government to play a significant role in promoting cyber security in Australia. It argues that the Australian Government should focus less on enhancing its own operational capabilities and more on supporting broader national activities, and identifies five key areas that should be addressed in a new Australian Government cyber security strategy.

Cyber Security: Time for an integrated whole-of-nation approach in Australia

Introduction

The digital age is central to Australia's national security and economic prosperity. From terrorism to organised crime to espionage, malicious cyber activity is a growing and ever changing national security threat.[1]

In the 2013 document *Strong and Secure: a strategy for Australia's national security*, the Australian Government identified 'malicious cyber activity' as one of seven key national security risks, and 'integrated cyber policy and operations to enhance the defence of our digital networks' as one of only three five-year priorities.[2]

The key cyber security announcement in the *Strong and Secure* strategy was the establishment of the Australian Cyber Security Centre, which is likely to be operational in early 2015 when the facility from which it will operate becomes available.[3] The *Strong and Secure* document has since been removed from the Department of the Prime Minister and Cabinet's website, in a signal that the Abbott Government wishes to set its own national security agenda. However, the establishment of the Australian Cyber Security Centre continues to have the Government's support.

While terrorism and specifically the Islamic State are dominating the national security agenda at the moment, cyber security is still an important issue for the Australian Government. It remains an issue that requires a continued commitment to address the threats and vulnerabilities to protect Australia's national security from malicious actors. These actors generally fall into one or more of five broad categories: cyber criminals, issue-motivated groups or 'hacktivists', trusted insiders, nation state-supported groups, and nation states.[4]

These actors generally seek to achieve one or more desired outcomes, including financial gain, highlighting a cause or gaining attention, unauthorised access to information or intellectual property, or denying, disrupting or degrading access to systems or information. Annex A ('Malicious Cyber Actors, Desired Outcomes and Examples of Cyber Threats') provides a table describing the five broad categories of malicious cyber actors and their desired outcomes, as well as a number of examples.

To understand why cyber security is still an important policy area for the Australian Government, it is useful to look at two key elements. First is the current economic costs and personal impacts that cyber crime has on businesses and individuals in Australia. Second is the potential impact of a cyber threat based on the levels of reliance that Australians have, both individually and collectively, on information and communications technology (ICT).

General Keith Alexander, at the time the Director of the US National Security Agency and Commander of US Cyber Command, stated in 2012 that the loss of industrial information and intellectual property through cyber espionage constitutes the 'greatest transfer of wealth in history'.[5] McAfee, a leading cyber security company, estimated that the cost of malicious cyber activity in 2013 was between US$300 billion and US$1 trillion or 0.3 to 1.14 per cent of global GDP (measured in purchasing power parity terms).[6]

Symantec, another leading cyber security company, estimated the cost to Australia in 2013 was US$1 billion or 0.1 per cent of GDP.[7] While 0.1 per cent of GDP does not sound high, it has the potential to grow sharply and it is still a loss of US$1 billion that could be greatly reduced through relatively-inexpensive government policies and activities.

At the micro or individual/firm level, Symantec estimates that 60 per cent of Australian adults have experienced cyber crime (compared with 61 per cent globally) and that the average cost per victim in 2013 was US$187.[8] CERT Australia (the Australian Government's Computer Emergency Response Team within the Attorney-General's Department), in its *2013 Australia Cyber Crime and Security Survey*

Report, reported that 56 per cent of organisations surveyed had suffered a cyber security incident in the previous 12 months.[9] Similarly, a 2014 report by the Ponemon Institute identified that 44 per cent of organisations surveyed globally had suffered a serious cyber security incident in the previous year.[10]

For a business, the cost of a cyber security incident or breach can vary based on both the tangible cost of responding to and recovering from the incident, and intangible costs such as reputation damage. Kaspersky, another leading cyber security company, estimated the cost to a large company averaged US$649,000 for each incident, while for a small or medium company it was US$50,000.[11] These costs, particularly for a small or medium company, likely represent a barrier to innovation and productivity; they certainly represent an opportunity cost to both the business and the national economy that is difficult to measure.

The potential costs of cyber threats resulting from a loss of confidence in using online services must also be considered. Australians are embracing the Internet as both a marketplace for the sale of goods and services, and as an increasingly important source of social interaction. The Australian Bureau of Statistics estimated in 2012-13 that 83 per cent of Australians were Internet users. The percentage of those who used the Internet for purchasing goods and services was 76 per cent, while of the 24 per cent who did not use the Internet for purchases, half identified concerns about security as the key reason.

In the same study, the Australian Bureau of Statistics identified that 72 per cent of Internet users transacted Internet banking and 66 per cent were active on social networking sites.[12] The National Australia Bank, in its *July 2014 Online Retail Sales Index,* valued online retail sales at A$15.6 billion or 1 per cent of GDP, with 76 per cent of this spending going to domestic retailers.[13] In March 2012, the Boston Consulting Group estimated that the Internet economy in 2016 will account for 1.7 per cent of Australia's GDP and 8.9 per cent of retail sales.[14]

What will be the effect on retail spending if people lose confidence in the convenience of online shopping? What will be the productivity impact of people no longer using Internet banking, instead going back to branches? What will be the effect on businesses which have invested heavily in online products and service delivery? What will be the effect on people's social relationships without online social networking? These questions, among many others, need to be considered when assessing the importance of cyber security.

The vulnerability of Australia's critical infrastructure to cyber threats must also be considered. In a global survey of more than 600 ICT and security executives from critical infrastructure providers, 54 per cent stated they had experienced large-scale attacks on their infrastructure. In Australia, more than 60 per cent of those surveyed believed foreign governments had been involved in attacks against critical infrastructure in Australia and, in a follow-up survey, 90 per cent of respondents in Australia were 'worried about their sector's vulnerability'.[15]

The connectivity of some sectors of critical infrastructure, particularly the power grid, is growing as new 'smart grid' projects are implemented. These systems allow two-way communication between the electricity company's systems and the individual devices, such as meters, via the Internet.[16] Alarmingly for critical infrastructure providers, researchers at the Freie Universität in Berlin have shown that it is possible to identify and interactively map Internet-connected supervisory control and data acquisition systems, such as those commonly used in critical infrastructure, which is information that could be very valuable to malicious cyber actors.[17]

'Cyber security' is the outcome of the activities and actions to protect against cyber threats and is generally implemented in a risk-based manner, addressing the most significant risks first. Cyber threats target a system, organisation or individual directly, and it is these entities that have primary responsibility for assessing their risk and implementing the appropriate cyber security solutions. However, threats against one organisation can have potential impacts on others.[18] These second-order victims, enabled by the interconnected nature of the Internet and modern business relationships, include business partners, customers and even unrelated businesses with shared customers. A significant example is that when the security company RSA was breached in 2011, the information

gained was used to breach the systems of Lockheed Martin, one of the largest defence contractors in the US.[19]

It is impossible for the Australian Government to directly provide cyber security capabilities for the entire business and civilian population. However, this paper will argue that the direct costs, the potential future impact, and the second-order effects of cyber threats require the Australian Government to play a significant role in promoting cyber security in Australia.

The paper will argue that the Australian Government should focus less on enhancing its own operational capabilities and more on supporting broader national activities in five key areas. First, by publishing a regularly-reviewed cyber security strategy to identify and prioritise the nation's activities to enhance cyber security. Second, by stimulating the Australian cyber security industry and encouraging demand for and supply of innovative, secure ICT services. Third, by providing incentives for government agencies and businesses to implement effective cyber security. Fourth, by enhancing the cyber security workforce through promoting cyber security careers to secondary and tertiary students. Finally, by undertaking effective international engagement to leverage and enhance the experience and expertise developed in other nations.

The paper will be presented across six parts. Part 1 will provide context for a new Australian Government cyber security strategy by analysing the current approach to addressing cyber threats. It will focus on the current roles and responsibilities of key areas of Australian government and business, and identify and analyse where issues, shortfalls and opportunities exist in the current approach. In Part 2, the paper will recommend that the Australian Government produces a new cyber security strategy as the key first step and will include a set of suggested objectives and strategic priorities.

Parts 3 to 6 will recommend initiatives for achieving four of the key new strategic priorities identified in Part 2. These have been designed to be low cost or cost neutral for the Australian Government and be cost effective in the benefits delivered, which is seen as critical in the current fiscally-constrained environment. Part 3 will focus on initiatives to stimulate demand and supply of services from the cyber security industry in Australia. Part 4 will focus on initiatives to achieve the strategic priority of enhancing the cyber security of key areas of Australian business. Part 5 will provide a suggested initiative to enhance the quantity and quality of the Australian cyber security workforce, specifically through engagement with the tertiary education sector. Part 6 will identify key initiatives for the Australian Government's diplomatic and international engagement on cyber security.

Part 1 – The current approach to cyber security in Australia

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.[20]

In Australia, like much of the world, the ICT systems that store and process sensitive personal and business information, and control critical national infrastructure, are owned and operated by a mixture of businesses, governments and individuals and their contracted service providers. Links between individuals and organisations are provided by Internet service providers (ISPs)—generally telecommunication companies—which provide the backbone networks, connectivity to the global Internet and access points for users.

Ultimate responsibility for the security of ICT systems is with the owner or operator of any system, as they have the greatest ability to influence its implementation. However, governments, ISPs and the cyber security industry can and do play a significant role in cyber security. Admiral Michael Rogers, the current commander of US Cyber Command and the National Security Agency, observed in July 2014 that:

> [C]yber is the ultimate team sport. There is no one single organisation that has all the answers, there is no one single technology that will solve all of our problems, meet all of our challenges.[21]

The role and approach of the Federal Government

In practice, the Australian Government has four key roles in cyber security. The two primary roles for government are to develop, implement and enforce cyber security legislation, regulation and policy, and to engage internationally on cyber security to promote coordination and cooperation in addressing cyber threats. The third role is the provision of policing to investigate cyber crimes and criminals. The fourth is to provide guidance, advice and some operational capabilities to identify, prevent and detect cyber threats.

The current focus of the Australian Government is the provision of information and resources to educate ICT systems owners, including businesses and individuals, on cyber security threats and vulnerabilities. Some key examples of the resources include the Australian Signals Directorate's 'Information Security References' page, CERT Australia's 'Advice' page, the Australian Federal Police's (AFP) 'Cyber Crime: Crime Prevention' page, the 'ThinkUKnow' campaign from the AFP and Microsoft, the Australian Communications and Media Authority's 'cyber(smart:)' site and the 'Stay Smart Online' site managed by the Department of Communications.[22]

The second focus of the Australian Government is its operational capability to identify and detect cyber threats, and respond where appropriate. This includes the investigation of cyber crimes by law enforcement, in particular the AFP's High Tech Crime Operations.[23]

Additionally, since the release of the 2009 cyber security strategy, the Australian Government has invested heavily in operational cyber security capabilities through the Cyber Security Operations Centre and CERT Australia. These organisations undertake activities to assist government agencies and business to detect cyber attacks or intrusions against their systems, and provide advice and assistance to respond to any such intrusions.[24]

The role and approach of state and territory governments

The state and territory governments in Australia have similar responsibilities but with a narrower focus on their respective constituents. In most jurisdictions, cyber security, particularly for individuals and businesses, is predominantly the domain of the local police force. The police focus on the identification, investigation and prosecution of cyber crimes and criminals, while providing some limited guidance to protect constituents from cyber threats.[25]

Education is the one area that state and territory governments can and do play a large role, not least because the delivery of public education in Australia is constitutionally the mandate of the states.[26] It is an important area that could be leveraged further to enhance the understanding of cyber threats and how to address them by all Australians, particularly young adults and children.

The role and approach of ISPs

ISPs are a special case in industry when it comes to cyber security. They play a unique role in providing the gateway to the Internet for Australian governments, businesses and individuals.[27] All traffic, both legitimate and malicious, flowing to and from ICT systems traverses one or more ISP's network. This privileged position provides the environment where ISPs could significantly enhance cyber security through the provision of 'secure' options for connectivity.

The ISP community already plays a role in this space. First, through its engagement with the AFP, it implement INTERPOL's 'Worst Of' list—used to block access to child abuse material for all ISP customers. Second, it voluntarily implements the Internet Industry Association and Australian Communications and Media Authority's i-code.[28] It encourages ISPs to identify malicious software infected computers on their networks and inform customers if their computers are infected, as well as providing advice and assistance on how to recover from the infection.[29] Additionally, a number of ISPs offer their home-based customers low-cost access to antivirus and other cyber security software to better protect them while online.[30]

The role of owners and operators of ICT systems

The owners and operators of ICT systems play the largest role in cyber security for two key reasons. First, they have the greatest ability to implement security in the system because of their access to and management of the system. Second, they have a duty of care to the users of these systems, who provide them with information to use their services. The key role of the owners and operators of ICT systems was a clear assumption in the Australian Government's 2009 cyber security strategy, where two of the three stated objectives were about businesses and individuals operating their own ICT systems securely.[31]

If all system owners implemented strong cyber security, malicious software would not be able to propagate as easily between systems, and Internet-connected systems would be a much harder target for malicious cyber actors. However, the cyber security capabilities of businesses and individuals, and their current implementation, vary greatly. While large businesses, such as banks, and defence industry and technology companies may have significant resources for cyber security and dedicated cyber security teams, small-to-medium enterprises often have no dedicated cyber security expertise, poor implementation and little budget.

The Australian Government and the cyber security industry provide a significant amount of guidance and educational material online, however, because they cannot access and influence all individuals and businesses directly, it is up to the business or individual to locate and implement the guidance. Moreover, notwithstanding its guidance and educational material, the Australian Government provides few policy, legal or regulatory drivers to encourage better cyber security among this group.

The Australian Government's current strategy

The Australian Government has released two cyber security strategies, the E-Security National Agenda, which was established in 2001 and reviewed in 2006, and the 2009 cyber security strategy.[32] The 2009 strategy identified six guiding principles, three objectives and seven strategic priorities to guide the implementation of an effective, integrated, whole-of-nation approach to cyber security.

While the principles, objectives and priorities identified in the 2009 strategy are logical goals for the Australian Government to pursue, it has had varied success in their implementation. The Government has undoubtedly taken action on cyber security since the 2009 strategy, with the establishment of both the Cyber Security Operations Centre and CERT Australia being key achievements.[33] However, there is little evidence that the Government has achieved significant gains in partnerships and shared responsibility, the key goals that make cyber security a 'team sport' and allow a whole-of-nation approach to cyber security.

CERT Australia has partnerships with over 500 businesses, however, the nature of those relationships is unclear.[34] Are they customer-provider or true two-way partnerships with shared responsibilities? Australia has also been active in international engagement on cyber security, both bilaterally and multilaterally. Australia has led and contributed to a number of working groups and reports being prepared by multinational institutions, such as the UN, and Internet governance organisations such as the Internet Corporation for Assigned Names and Numbers, and the International Telecommunications Union.[35]

The proposed new Australian Cyber Security Centre aims to 'improve partnerships between governments and with industry', with the view to 'see[ing] more seamless interaction with international and industry partners'.[36] It will bring together the Australian Government's key operational cyber security organisations, namely CERT Australia, ASIO's Cyber Espionage Branch, elements of the AFP's High-Tech Crime Operations and parts of the Australian Crime Commission.[37]

Having these organisations together, and coordinating their engagement internationally and with businesses and academia, will almost certainly assist the Australian Government to engage more effectively.[38] However, it remains to be seen how the decision to house the Australian Cyber Security Centre within ASIO's new 'high-security' facility in Canberra affects its ability to effectively engage with industry.[39]

Part 2 - A new and periodically-reviewed cyber security strategy

The 2009 cyber security strategy was an excellent first cyber security strategy for Australia. But Australia's use of ICT, its key vulnerabilities, and the threats seeking to exploit those vulnerabilities have moved on since 2009. Five years after the last strategy, and with a new Australian Government with new priorities, it is the ideal time for a new cyber security strategy. It should be used to signal a shift in focus from enhancing the Government's own cyber security capabilities to establishing effective domestic and international partnerships in cyber security and promoting an environment of shared responsibility.

The Australian Government should use the new cyber security strategy to identify and coordinate the policy, legislative, regulatory, diplomatic and operational activities of Australian Government agencies. The strategy, managed by the Department of the Prime Minister and Cabinet as the cyber policy lead, should ensure activities across the Australian Government are consistent and working to achieve a whole-of-nation approach to cyber security.

The objectives for a new cyber security strategy

The new cyber security strategy should include a new set of objectives that reflects the Australian Government's desired outcomes with respect to cyber security. Each of these objectives should be considered equally important. While each in isolation would deliver benefits to the nation, their complementary nature means the benefits will be far greater when implemented as a package.

Objective one should be that 'Australian businesses and individuals secure their systems and are able to transact online safely and securely', reflecting that the desired outcome is not just an awareness of the risks but also that something has been done about them. Objective two should be that 'Australian Government and critical infrastructure providers will be a hard target or target-of-last-resort for malicious cyber actors'. This objective reflects that while cyber threats will always remain, Australian Government and critical infrastructure systems will need to make the job of sophisticated cyber actors significantly more difficult.

Objective three should be that 'Australia's cyber security industry will be able to provide innovative, effective and efficient services to assist the Australian Government, businesses and individuals to secure their systems'. This reflects the desired outcome of partnerships and shared responsibility with the cyber security industry. Objective four should be for 'Australia to be a leader in international cooperation and engagement on cyber security and cyber crime', reflecting that the Government recognises that cyber threats are a global issue and that the international community can work together to address the threats more effectively. Objective five should be that 'all Australians are educated on cyber threats and act to protect themselves'. This would reflect that the Government recognises the need to educate its citizens on cyber safety and security, and that the education sector plays a key role in cyber security.

Strategic priorities for a new cyber security strategy

With a new set of objectives defined, the strategic priorities should be developed accordingly. It is suggested that these priorities should be:

1. Australian businesses and individuals to be able to access appropriate information and guidance on the identification, detection and prevention of cyber threats.

2. The Australian cyber security industry be supported to enable it to provide, innovative, efficient and effective cyber security capabilities and services.

3. Australian Government and critical infrastructure systems to implement minimum standards to identify, protect, detect and respond to cyber threats.

4. Australia to work with international partners and multinational institutions to ensure that cyber crimes can be efficiently investigated and prosecuted regardless of the source or destination.

5. Australia to identify opportunities to cooperate internationally on cyber security and to define rules and norms for state behaviour and responsibilities in cyber space.

6. The Australian Government to work with the education sector to ensure that effective cyber safety and security modules are delivered to students.

7. The Australian Government to implement and maintain capabilities to assist all levels of government, as well as businesses and individuals, to deter, detect, respond and recover from sophisticated cyber threats.

8. The Australian Government to work with the tertiary education sector to develop an effective cyber security workforce.

In the remainder of this paper, four of these strategic priorities will be expanded on to outline the key initiatives that should be undertaken to achieve these priorities. The Australian Government's new cyber security strategy should provide specific initiatives to achieve its stated objectives and implement its strategic priorities, which need to represent implementable and measurable commitments. The 2009 cyber security strategy had few such initiatives, making it difficult for the Australian Government to measure and report on its performance and effectiveness in implementing the strategy.

Part 3 - Initiatives for stimulating the Australian cyber security industry

These initiatives represent the key change of focus for the new cyber security strategy. They relate to the strategic priority of stimulating demand and supply of innovative, efficient and effective cyber security solutions and capabilities. Australia has a vibrant and expanding cyber security industry, however, more needs to be done to stimulate demand for its services and to increase the incentives for the companies involved to innovate.

It is worth noting that the Australian Information Security Association has more than 2000 members, while the International Information Systems Security Certification Consortium—an organisation that certifies information security and risk professionals globally—has 1795 Australian members; also, CREST Australia, a certification body for security assessors, lists 17 companies with one or more CREST-certified assessors.[40]

To stimulate demand, the Government should implement regulations or provide incentives to businesses to improve their cyber security. Regulations could include placing an additional cost on a business for not implementing adequate cyber security, or providing an additional benefit where they have implemented good cyber security. That said, the incentive approach can be difficult, as it is hard to prove the negative in cyber security, where the absence of a breach or compromise does not necessarily indicate good cyber security; it could be luck or it could be that the business or individual has been compromised and does not know it.

Specifically, the Australian Government should look at two key low-cost initiatives. First, the introduction of data breach notification laws for publicly-listed companies and businesses that store and process personal information. Second, an expansion of the current Australian Internet Security Initiative to place mandatory membership and mandatory actions on ISPs for detecting and isolating compromised hosts using their services.[41]

Mandatory data breach notification laws

Data breach notification laws, that is the requirement to report to a regulator and/or data owner when a compromise or breach occurs, place reputational and ultimately financial pressure on businesses and companies to maintain effective cyber security and minimise the likelihood and impact of a data breach. Such laws have been enacted extensively in the US. For example, 47 US states (including Washington DC), Guam, Puerto Rico and the Virgin Islands have implemented mandatory data breach laws.[42] Australian Government agencies similarly already have a requirement to report breaches to the Australian Signals Directorate, being the Government's information security authority.[43]

To get the most benefit upfront, the Australian Government should focus on publicly-listed companies and those that store and process personal information of their customers. The companies with personal information are likely to be targeted and a breach is likely to affect many people. They also represent a section of industry that can be regulated easily through existing bodies such as the Australian Securities and Investment Commission.

Publicly-listed companies currently have a large incentive to cover up data breaches because of the potential effects on stock value. The future value of a company and therefore the returns to a shareholder are often linked to their intellectual property (for example, the recipe for Coca Cola or Big Mac Sauce, or the plans for sophisticated technology such as the Joint Strike Fighter aircraft), which may be their market differentiator. The Australian Signals Directorate reports that malicious cyber actors frequently target intellectual property as a key driver or outcome of a breach or compromise.[44]

The Australian Government should implement laws or regulations that require publicly-listed companies to report any cyber breach which results in a loss of data. These reporting requirements place indirect costs, particular as the media becomes aware of the issue, on companies and businesses that suffer a breach. These costs strengthen the incentives to invest in cyber security to prevent the reputational and resulting financial impacts of a data breach.

The reports should be made to the AFP (for investigative purposes), the Australian Securities and Investment Commission as the market regulator, and the Australian Stock Exchange for inclusion in market news so that shareholders can make investment decisions accordingly. In addition, all companies that suffer a breach of personal information of customers or business partners should be required to report the breach. Breach reports in this instance should go to the Office of the Australian Information Commissioner and directly to the customers or business partners affected.

There is a counter argument against mandatory breach reporting that argues it will lead to 'wilful blindness' and 'disincentive for some to actually know what is going on'.[45] However, it could be argued that, at worst, this 'wilful blindness' already occurs or, at best, that many companies currently do not understand the impact of cyber security breaches and therefore the benefits of strong cyber security. Implementing the mandatory reporting requirements would raise the awareness of those that do not understand the cyber threat through the external regulation and incentives.

For those that are wilfully blind to the issue of cyber threats or simply choose to ignore them and not report, the Government could complement the mandatory notification laws with a protected whistle-blowing scheme. The AFP or regulatory bodies (such as the Australian Securities and Investment Commission or the Office of the Australian Information Commissioner) would investigate accusations of non-compliance, and the courts could impose significant fines or prosecute the executives of companies which fail to meet their mandatory reporting obligations, as is already common with workplace health and safety laws.[46]

To implement these changes, the AFP, the Australian Investment and Securities Commission and the Office of the Australian Information Commissioner would need their staffing levels augmented to collect, process and action the data breach notification reports. It could be expected that this would be approximately ten Australian Public Service (APS) staff (four APS-level 4, four APS-level 6 and two executive level one), split evenly between the Australian Investment and Securities Commission and the Office of the Australian Information Commissioner, and five AFP officers. Using the current Department of Finance's costing template for APS staff, this would equate to an additional $1.8 million per year, including both direct remuneration and staff on-costs.

In addition to the staffing costs, the responsible agencies would need to undertake an advertising and awareness campaign for potentially-affected businesses. The campaign would need to be in compliance with guidelines produced by the Department of Finance.[47] The final costs would depend on the form of advertising chosen, however, it would need to be sufficiently broad to ensure potentially-affected businesses are aware of their obligations. Based on the costs of a similarly campaign by the Department of Immigration and Citizenship in 2012-13, it could be expected to cost around $700,000.[48] Finally, this initiative may require the relevant agencies to approach the market for the development of the systems and processes to support the reporting and processing activities. This would need to be confirmed with the responsible agencies.

Expanding and mandating the Australian Internet Security Initiative

The second initiative to stimulate the cyber security industry would be to expand the current Australian Internet Security Initiative. Under the current initiative, run by the Australian Communications and Media Authority, ISPs are provided with reports of activities on their networks that are common in compromised or malicious systems.[49] The ISP can take action to notify the customer, and isolate or remediate the system. However, the actions of the ISP are not mandated or regulated by the initiative, although another voluntary code, the Internet Industry Association's iCode, does provide guidance and recommendations to ISPs.

The new initiative should strengthen this process by making membership of the Australian Internet Security Initiative mandatory for ISPs. Currently, the initiative's 139 members cover 90 per cent of Australia's Internet traffic.[50] In addition to making it mandatory to be a member, the initiative should mandate actions to be taken by ISPs when they are informed of compromised systems on their networks. This should include a tiered approach of notification to the owner, to isolation of the affected system until it is remediated.

By placing a larger burden on the ISPs to ensure their customers are not negatively impacting the cyber security of others, the Australian Government would encourage the ISPs to offer secure services to their customers. The incentive for customers to purchase these secure services is that their systems may be removed or isolated from the network if they are not appropriately secured and are subsequently compromised. The incentive for the ISP would be reputational; if an ISP can show that using their secure service resulted in less time removed or isolated from the Internet, it provides an incentive for ISPs to compete on security, not just speed and cost.

The implementation of this initiative, other than to draft the necessary legislation, should be cost neutral to the Australian Government. It would have a significant effect in highlighting the importance of key partnerships between owners and operators and service providers in cyber security, and stimulate demand for innovative secure solutions from ISPs. However, significant care would need to be exercised in drafting the legislation to minimise the risk of the Australian Government being accused of limiting business opportunities and restricting trade of companies should they be removed from the Internet.

Part 4- Initiatives for improving the cyber security of Australian business

The Australian Government will need to prioritise its direct effort on cyber security towards the security of those systems that are most likely to be targeted, and which would cause the Australian Government and the Australian public the most damage should they be breached or attacked. The capabilities and resources of the Australian Government, particularly those within the proposed Australian Cyber Security Centre, are impressive but they cannot possibly stretch to protect all Australian ICT systems all of the time.

Under this prioritisation, the Australian Government should focus on systems that support Australia's critical national infrastructure and the systems of the Australian Government itself. While breaches and attacks of the systems of a majority of businesses may have economic and financial impacts for the business, it is unlikely to be an issue with significant national implications. On the other hand, if critical infrastructure and Australian Government systems are compromised or rendered unavailable, the

delivery of essential services could cease, with consequences that affect national governance and the health and safety of citizens.

Minimum cyber security standards for government and critical infrastructure systems

To make these systems more resilient, the Government should develop and mandate minimum cyber security standards for Australian Government and critical national infrastructure systems. The Australian Government already has the basis of the minimum standards in its *Information Security Manual*, produced by the Australian Signals Directorate, which is mandatory for Australian Government agencies. [51] The *Manual* is currently heavily focused on securing government systems, and the standards are based on the security classification of information, which often means little to the private sector.

To support the new minimum standards, the *Information Security Manual* should be rewritten to make it more applicable for non-government organisations. This could be achieved by documenting the mandatory protections based on a threat and level of risk, rather than the classification of the information it stores or processes. This risk-based ordering would aid both government and non-government organisations to assess their cyber security implementation against their threat environment. It would enable the Australian Government to recommend, and organisations to apply, protections above the minimum standards if the threat environment warrants.[52]

The Australian Government would need to establish the appropriate law or regulations to mandate the standards, and the associated performance reporting and compliance, and auditing regimes to enforce the law or regulation. To achieve this, the Australian Government would need to create a new national security law focused on cyber security for critical infrastructure. It would need to articulate what the government considers critical infrastructure, and detail the authoritative document(s) for the standards.

The Rudd/Gillard Government produced a Critical Infrastructure Resilience Strategy in 2010 that provided a high-level definition of 'critical infrastructure', however, to enforce the minimum cyber security standards, a definition that allows for less interpretation is required.[53] The new law needs to place requirements on the operators of critical infrastructure system to report annually their compliance with the developed standards, and provide evidence of independent audit and risk assessment against the compliance. To complement the standards and compliance regime, the law should also specify penalties for failing to report or non-compliance.

The responsibility for reporting, compliance and monitoring regimes should be placed with the Attorney-General's Department, which has coordination responsibility for critical infrastructure resilience for the Australian Government.[54] The development and maintenance of the cyber security minimum standards should be undertaken by the Australian Cyber Security Centre, utilising the existing expertise of the Australian Signals Directorate in standards development and the expertise of CERT Australia and ASIO in critical infrastructure security.

The creation and maintenance of the standards could be undertaken under existing resourcing, as part of the regular *Information Security Manual* review cycle. The reporting, compliance and monitoring regime would likely require CERT Australia to be augmented by up to five APS staff, such as two APS-level four, two APS-level six and one executive level one staff member. Using the current Department of Finance costing template, this would equate to an additional $620,000 per year, including both direct remuneration and staff on-costs. In addition, the Attorney-General's Department would need to undertake an advertising and awareness campaign for potentially-affected businesses.

Advertising for this initiative would similarly need to be in compliance with Department of Finance guidelines.[55] The final costs would obviously depend on the form of advertising chosen but, again, would need to be sufficiently broad to ensure that potentially-affected businesses are aware of their obligations, and could be expected to cost around $700,000.[56]

Cyber security threat and knowledge sharing

Most cyber threat actors do not target a single business or agency. Even so-called 'advanced persistent threats' often target multiple business in multiple industries, using the same or similar tools, techniques and procedures.[57] Hence combatting these threats could be enhanced through the sharing of actionable cyber threat intelligence and knowledge between organisations. By sharing, many could benefit by using the experience of others. The Australian Government should play a role in supporting the establishment of the agreements, systems and processes to enable timely and actionable intelligence and knowledge sharing.

The Australian Government has previously established the Trusted Information Sharing Network to enable sharing of 'vital information on security issues relevant to the protection of our critical infrastructure and the continuity of essential services in the face of all hazards'.[58] The network includes a number of sector-specific groups, to enable the sharing of information within a sector, and a small number of expert advisory groups, including one for cyber security, which can advise across all the sector specific groups.[59]

The cyber security advisory group has produced a number of publications providing guidance for network members and the general public.[60] While the network provides a great forum for the sharing of high-level threat information, it does not readily enable the sharing of technical information or detailed intelligence with other organisations to detect and respond to cyber attacks or compromise.

The Australian Government, with the support of an industry partner and the network's existing cyber security expert advisory group, and in consultation with relevant sectoral groups, should develop a pilot or prototype system (including policy and processes) to securely share technical details of threats and the detection rules and response options to defeat them. In the US, many of the sectoral 'Information Sharing and Analysis Centers', which are roughly equivalent to Australia's network sector groups, have established cyber information sharing systems and processes.[61]

These centres are run by members and jointly funded by members and the US Government. Once the Australian Government and industry partner have developed a pilot or prototype system, the industry partner would be able to offer the solution to a sector group either as a fee-for-service or as a licensed software (and hardware) system. The Australian Government would ideally have provided the seed funding for the innovation, allowing the industry partner to reduce the cost for the service or system offered to the sectoral groups.

At that point, funding and steering of the sectoral cyber threat and knowledge sharing centres should be from members, who could offset the cost with reducing their own internal cyber security capabilities. The Australian Government could look to fund these cyber threat knowledge sharing centres in the future if they do not receive the necessary support and commitment from business, albeit that should be considered a last resort.

The Australian Cyber Security Centre should negotiate with the sectoral groups to provide the Government's shareable threat information into the sector group systems, further strengthening the business and government partnership for cyber security. It should also investigate whether sectoral groups are willing to provide a feed of threat information back to government to assist in its own situational awareness of the cyber threat. However, while this would be desirable, it should not be pursued if it represents a barrier to businesses within a sectoral group from participating because of concerns about sharing commercial information with government.

The cost of this proposal for the Australian Government would be in establishing the pilot or prototype system (and policy and processes) with the industry partner. The cost is difficult to quantify, as it would depend on negotiations with the industry partner about its ability to commercialise the solution being developed. If the Australian Government is successful in stimulating demand for cyber security services and capabilities through other initiatives, demand for the jointly-developed service or system would be enhanced. If the Government could encourage each of the sectoral groups to implement the solution, and the industry partner was able to sell it more broadly, the business case for the industry partner to lower or waive the upfront cost to government would be significantly improved.

Part 5 - Initiatives to enhance the cyber security workforce

Technical capabilities are important for effective cyber security. However, having the right professionals to identify and analyse threats and to develop, implement, maintain and monitor cyber security capabilities is critical to their effective operation. In recent times, cyber security professionals have been in high demand both in government and industry, and it has been observed that Australia, like much of the world, faces a cyber security skills shortage.[62]

National ICT Australia has warned that 'Australia could miss the chance to build an internationally competitive cyber security industry if it doesn't … create market opportunities and challenging careers for our best computer scientists and software engineers'.[63] To address this, the Australian Government should increase its activities to assist tertiary institutions in promoting cyber security as a rewarding and valuable career path for the best and brightest ICT students.

Promoting cyber security as a profession with students

In 2012, the Australian Government, in partnership with Telstra, delivered the first Cyber Defence University Challenge for 17 teams of undergraduate students from Australian universities. Since 2012, the challenge has expanded to 55 teams from 22 different tertiary institutions.[64] Renamed the Cyber Security Challenge Australia in 2013, the challenge aims to 'excite, inspire, attract and help Australia's talented people to become our next generation of cyber security professionals'.[65] The challenge tested key cyber security skills, such as vulnerability assessment, penetration testing, and computer and network forensics. Participants undertake challenges in each of these areas and are shown a range of prospectively-exciting careers in cyber security.

The Australian Government should expand on the success of these challenges to include a challenge for Year 11 and 12 students. The aim would be to encourage the take-up of ICT and cyber security courses at university, rather than pursuing other disciplines.[66] By limiting the challenge to current ICT students at university, an opportunity may be lost to influence prospective ICT students to enrol in ICT and cyber security courses and, potentially, to increase both the quantity and quality of students studying cyber security.

Further to that, the current Cyber Security Challenge Australia should be expanded to become a two-part challenge involving a regionally-based qualification tournament and national finals. By holding a regionally-based qualification tournament, more tertiary institutions would be able to compete with more teams and a greater number of students would be influenced on the career opportunities available in cyber security.

The universities would benefit through the ability to benchmark themselves against like universities and implement incremental improvements to their cyber security programs, rather than comparing themselves to larger and more affluent universities with existing strong cyber security programs. After the qualification step, the best performing teams should be selected from each state and territory to compete in the national finals for the major prizes.

Implementing the expanded challenge should become a priority for the new Australian Cyber Security Centre. It contains all the necessary Australian government skills and expertise and, most importantly, has the key role in establishing and maintaining the Australian Government's relationships with industry on cyber security. While much of the current work to implement the Cyber Security Challenge Australia is being performed by the Australian Signals Directorate and CERT Australia, the Australian Cyber Security Centre could use the challenge to engage with industry to play a larger role for the benefit of the government, industry, universities and the students.

Having the cyber security industry playing a larger role would also provide a greater opportunity for it to engage with and recruit the brightest talent in cyber security. For students, this would enhance their opportunity to impress prospective employers and provide a vehicle to secure employment. The universities could use a good performance in the challenge by their team(s) as a differentiator to attract the best and brightest students and, potentially, to attract industry partners or provide a focus on key areas they need to improve their course.

The benefits for the Australian Government are both direct and indirect. Increased industry engagement would lighten the burden on the Government's skilled professionals for other duties, while the increased competition between the universities should lead to a greater focus on cyber security and, ultimately, better educated and trained cyber security graduates.

Expanding Cyber Security Challenge Australia in this way would represent no additional cost to the Australian Government and, indeed, is likely to be cheaper than the current arrangement. The initiative would enable the cyber security industry to play a more prominent role, to the benefit of all involved. For the Australian Government, less direct commitment would be required as its role shifted from design, implementation and management to supporting an industry partner to deliver the outcomes.

Part 6 - Initiatives for the Australian Government's international engagement and diplomacy

The Internet connects nations closer than ever before and provides great opportunities to trade, share, influence and communicate with neighbours both near and far. At the national level, cyber space provides an environment where interstate competition and conflict can occur and diplomatic tensions can be increased. But it also creates opportunities to enhance Australia's diplomatic engagement and cooperation to address a common and shared problem.[67] Australia should capitalise on this opportunity to cooperate internationally and seek ways to mitigate the cyber threat to Australia, and enhance our bilateral and multinational relationships.

The Department of Foreign Affairs and Trade (DFAT), in its role of advancing the interests of Australia and Australians internationally, has already placed cyber security on the agenda in a number of bilateral agreements and multinational institutions.[68] The current Australian Government has also sought to add cyber security to the agenda in a number of bilateral discussions: in 2013 and 2014, for example, Australia established dialogues or cooperation on cyber security with India, Indonesia, the Republic of Korea and Japan.[69]

In addition to the DFAT-led initiatives, Australia's operational cyber security agencies play an important role in international engagement. CERT Australia is active in the international 'computer emergency response' community, particularly through its membership in the Asia Pacific Computer Emergency Response Team.[70] The Australian Signals Directorate also has close intelligence and operational response relationships with its equivalent agencies in the US, UK, Canada and New Zealand.

However, despite significant activity in international engagement on cyber security, there does not appear to be an overarching strategy or plan that guides Australia's approach. It is, therefore, difficult to determine if there are gaps, overlaps or even conflicting activities being undertaken across the Australian Government. To address this, and to ensure its international engagement is both efficient and effective, DFAT should develop an international engagement and diplomacy plan for cyber security.

Developing an international engagement strategy was identified as an activity in the 2009 cyber security strategy, however, there is no evidence it was ever completed.[71] In particular, the plan should address four key areas. First should be the development and implementation of international laws and norms or behaviour in cyber space. Second is the sharing of cyber security threat intelligence and incident response cooperation. Third is cyber security capacity building in the Asia-Pacific region. Fourth would be cooperation on the investigation of cyber crimes and the prosecution of cyber criminals.

International law and norms of behaviour in cyber space

Despite cyber threats being a truly international problem, there are no international agreements on a nation's responsibilities with respect to cyber crime and cyber security. While the UN affirmed in 2013 that existing international law applies to a state's use of cyber space, the closest thing to a broad agreement between nations is the Council of Europe's Convention on Cybercrime.[72] To date, only 54 of the 193 nations in the UN have signed, ratified or acceded to the convention, mostly from Europe. [73]

While this commitment is commendable, it still leaves the majority of nations across the globe outside the agreement.

In September 2011, China and Russia surprised the international community by submitting a proposal to the UN General Assembly outlining an 'International Code of Conduct for Information Security'.[74] Unfortunately, the proposal has drawn criticism from the US, in particular, for two key reasons. First is its focus on information security rather than cyber security, which is seen by the US as justification for restricting the access of citizens to information. Second, the proposal places great emphasis on the right of a state to control information and combat cyber threats against it, without clearly articulating the state's role, responsibility and accountability in preventing cyber threats that originate within its jurisdiction.[75]

The creation of an UN-supported international code of conduct, or an agreed set of norms of behaviour, is in Australia's interests and should be a priority for Australia's diplomatic engagement on cyber security. A code of conduct or agreed norms would articulate international expectations on how a nation state behaves in cyber space, and its role and responsibility with respect to preventing, responding to and prosecuting malicious cyber actors.

An international code of conduct would provide the basis for a nation to hold another to account diplomatically for its actions in cyber space and provide a basis for diplomatic or economic sanctions or, in the worst case, escalation to military activities. It is important to recognise that an international code of conduct would not be a panacea for preventing global cyber threats. The difficulty of attribution in cyber space, as well as the difficulty in proving a nation state's complicity in a cyber attack or compromise, means that any code of conduct or international agreement is unlikely to be legally enforceable.

While US concerns about the Chinese and Russian proposal are justified, and likely shared by Australia, Australia should seek to work with China and Russia to progress a code of conduct to an agreeable conclusion. DFAT is already actively engaged in this activity, which represents no additional cost to the Australian Government and should be elevated to a priority task for Australia at the UN. By playing a more active role in driving a solution on cyber security norms, Australia would continue to show leadership both in cyber security and the UN.

Cyber security threat intelligence sharing and incident response cooperation

The CERT-CERT relationships maintained by CERT Australia provide an excellent opportunity for cooperation on incidents affecting multiple nations, and for joint training and exercises. Cyber security is a global issue with many nations facing similar cyber threats. This common threat environment means that like-minded nations would benefit from cooperation and frequent information sharing. The near real-time sharing of information on threats targeting a nation's systems may provide another nation with the detail it needs to identify and prevent current or future threats.

While arrangements are in place to share classified information between Australia and its partners through the relationships operationalised by the Australian Signals Directorate, opportunities to expand sharing to other friendly countries which share similar threats should be explored. While it is true that information sharing needs to be approached with caution to ensure that it is not used against Australia, this caution should not artificially limit sharing with those where mutual benefit is possible.

The Australian Cyber Security Centre, with oversight from DFAT, should prepare a plan for cyber security information sharing with international partners. It should establish what data the Australian Government is willing to share, with whom, and in what format and timeframes. The plan should also identify what joint training and exercise arrangements agencies are willing to pursue.

For some nations, the Australian Cyber Security Centre may be willing to share detailed technical information on cyber threats detected and undertake joint training and exercises, while for others it may include only general information on cyber threats observed and recommended mitigations to address them. The Australian Cyber Security Centre and DFAT would need to play an active role in the plan's development to ensure agencies do not default to restrictive classification regimes without exploring all the possibilities for sharing. The resulting plan could be used by DFAT when undertaking

bilateral or multilateral diplomatic activities to identify mutually-beneficial agreements to further Australia's interests internationally.

This initiative is already the responsibility of the Australian Cyber Security Centre and its member agencies and does not represent any additional cost to the Australian Government. However, the establishment of the Australian Cyber Security Centre provides the Australian Government with an opportunity to challenge existing agency-based thinking on what can and should be shared, and approach the question from a whole-of-government perspective.

Cyber security capacity building in the Asia-Pacific region

The current Australian Government has yet to commit to a detailed strategy for Australia's national security. Prior to the election, it committed to a foreign policy of more focus on the Asia-Pacific region, highlighted by the slogan 'more Jakarta and less Geneva'.[76] In support of this policy, the Australian Government should seek to enhance its engagement on cyber security in the region.

The Australian Government should develop a plan to prioritise and engage with Asia-Pacific nations to assist them to enhance their cyber security capabilities. While this would provide a benefit for the recipient nation, it is also in Australia's interests. Malicious cyber actors, particularly so-called 'advanced persistent threats', often use 'hop' points in other nations through which they route their malicious activities. These 'hops' are established in countries where the victim may have a more implicit level of trust (or less mistrust), and are used to hide the true identity or location of the malicious actor.[77]

Providing advice and assistance to regional neighbours on cyber security may reduce the occurrence of that nation being used as a 'hop' point, and provide the Australian Cyber Security Centre and the cyber security industry greater opportunities to identify the true source of an attack. Additionally, the global nature of the activities of the Australian Government and Australian businesses means that their sensitive or valuable information is often located on systems in the very countries that would be the beneficiary of Australia's advice and assistance.

In April 2014, the Australian Strategic Policy Institute (ASPI) released a report titled *Cyber Maturity in the Asia-Pacific Region 2014* that sought to objectively rate the maturity of nations in the Asia-Pacific region based on 'the presence, effective implementation and operation of cyber-related structures, policies, legislation and organisations'.[78] ASPI also identified a 'cyber engagement scale for government and industry' that can be used as a reference tool for 'identifying opportunities for the sharing of best practice, capacity building, development and business opportunities'.[79]

The Australian Government should use ASPI's work to engage with those nations with a level of maturity that indicates they can effectively use any advice or assistance Australia provides. While improving cyber security in all Asia-Pacific nations is an admirable goal, it is unlikely to be cost effective, value for time and money, nor achievable. The type of advice and assistance provided would differ for each nation. It may be as simple as providing advice or assistance on policy, procedures or structures or it could involve providing capabilities or in-line advisors. The Australian Government has the opportunity to tailor the program based on affordability and to fit with existing priorities of international engagement and development assistance.

International cooperation on the investigation and prosecution of cyber crime

Criminals have been quick to take advantage of the global nature of cyberspace and embrace the opportunities that the interconnectedness of ICT systems and networks provides. While in the physical world a criminal is generally restricted to committing a crime where they are located, this is not the case in cyber space. A cyber criminal in Russia can easily commit a crime in Australia or the US, which for law enforcement represents a significant challenge.

The basic questions of where the crime is committed, that is, whose jurisdiction, whose laws apply and who will prosecute become much more difficult in international cyber crimes. Even when jurisdiction

is determined, investigating a cyber crime where the perpetrator and the victim may be geographically separated by half a globe and speak different languages is a further complication.[80]

To address these issues and difficulties, it is critical for Australian law enforcement, in particular the AFP, to foster cooperative relationships with law enforcement agencies across the globe.[81] As one of the nations that has acceded to and/or ratified the Council of Europe's *Convention on Cybercrime*, Australia participates in a 24/7 global network of high-tech crime points of contact which allows for speedy assistance between signatory countries.[82] However, given that only 54 nations have signed up to the convention, the vast majority of nations require either a bilateral or multilateral agreement to ensure there is mutual assistance between police to investigate cyber crime.

Australia is currently a party in 25 bilateral treaties.[83] However, the processes for mutual assistance are cumbersome and bureaucratic. The Attorney-General's Department has noted that requests for assistance 'can vary from a few days or weeks in very urgent cases to several months or years in cases which require the collection of extensive material, or which relate to complex investigations'.[84] These timeframes mean that the investigation of multinational cyber crimes and their prosecution, in most cases other than those considered 'very urgent', becomes impractical.

To address this issue, the Australian Government should prioritise within its international engagement and diplomacy, encouraging more nations to accede/ratify the *Convention on Cybercrime* or a similar agreement. The convention includes agreed actions to provide timely support of international cyber crime investigations. Where a nation cannot or will not accede/ratify the convention, Australia should seek a bilateral agreement with that nation, although that is clearly not the preferred approach. This activity should be led by DFAT, with support from the AFP and the Attorney-General's Department, and be undertaken as part of normal diplomatic engagement. As such, it would not require additional funding or resources.

Conclusion

The digital environment is becoming increasingly important to Australia's security and prosperity. At the same time, Australia faces cyber threats from a range of malicious actors, including cyber criminals, issue-motivated groups or hacktivists, trusted insiders, nation state-supported groups and nation states themselves. Malicious cyber actors seek to achieve one or more outcomes when undertaking their activities, including financial gain, gaining attention for a cause or issue, access to classified information or intellectual property, or to disrupt, deny or degrade ICT systems or information for legitimate users.

The combination of the increasing reliance on ICT for Australia's prosperity, the evolving cyber threat environment, the economic and reputational costs of cyber threats, the need to identify fiscally-restrained government initiatives to enhance cyber security, and the opportunity for the current Australian Government to put its own stamp on this issue means the time is right for the Government to develop a new cyber security strategy for Australia.

Since the 2009 cyber security strategy, the Australian Government has enhanced a number of its own capabilities to address cyber security threats, in particular by establishing two critical operational capabilities in the Cyber Security Operations Centre and CERT Australia. Additionally, in 2013 the establishment of the Australian Cyber Security Centre was announced to bring together operational cyber security agencies to ensure effective and efficient cooperation and engagement with the broader community.

This paper has argued that while the Australian Government has taken significant steps to enhance its own cyber security capabilities, it has not provided the environment that enables it to partner with and leverage the skills and capabilities of other areas of the Australian and international communities.

The Australian Government should issue a new cyber security strategy that shifts its focus from what the Australian Government should do to enhance its own cyber security capabilities, to what the Australian Government should do to enable the cyber security industry, business and critical infrastructure providers and universities to provide a more effective contribution. Additionally, the

new cyber security strategy should articulate how Australia will engage with the world to both leverage and provide expertise to address a truly global issue.

This paper has argued that the Australian Government should implement new policies, legislation and regulation to encourage Australian business, the cyber security industry (including ISPs) and critical infrastructure providers to be more proactive in developing or procuring innovative cyber security solutions. This includes implementing four key initiatives. First, introducing mandatory data breach notification laws for publicly-listed companies and businesses that hold personal information of customers and business partners. Second, expanding and mandating the current initiative for ISPs to detect and isolate computers exhibiting malicious behaviour. Third, implementing mandatory cyber security standards for government and critical infrastructure systems. Finally, establishing systems, policies and procedures for the sharing of cyber security threat intelligence and knowledge.

The Australian Government should also refine its approach to enhancing the cyber security workforce in Australia through engagement and cooperation with both the tertiary education sector and the cyber security industry. The Government should implement key initiatives to engage with tertiary education, with the support of the cyber security industry, to promote cyber security as a valuable and rewarding career for students and to encourage institutions to improve the standard and focus of their cyber security courses.

It has also been contended that the Australian Government should review the aims and focus of its international engagement on cyber security and ensure that these activities are given a high priority diplomatically. With cyber threats being a truly global problem, with no respect for national borders, mutual and real benefits are available through cooperation and coordination on cyber security. Key areas of focus for diplomacy and international engagement include the development and implementation of cyber norms, cyber security threat intelligence sharing and joint exercises, cyber security capacity building in the Asia-Pacific region, and international cooperation on the investigation and prosecution of cyber crime.

This paper has identified a number of low-cost or cost-neutral initiatives the Australian Government should pursue to enhance cyber security in Australia. In general, with some refining of approach and priorities, the majority of initiatives identified are achievable within existing organisational structures and resources.

The initiative to encourage cyber security threat and intelligence sharing would seek to partner with an industry provider to share innovation and minimise costs to the Australian Government. It is expected that this initiative could be delivered at zero financial cost (with some in-kind contributions) to the Australian Government. The initiatives to introduce mandatory data breach notification and mandatory cyber security standards would require additional ongoing APS and AFP workforce to manage the delivery of the initiatives and the delivery of advertising and marketing campaigns to ensure businesses are aware of their new responsibilities. Across both initiatives, the total cost in the first year would be approximately $3.8 million, with a recurring $2.4 million per year in subsequent years.

Annex A: Malicious Cyber Actors, Desired Outcomes and Examples of Cyber Threats

Malicious Cyber Actor	Description	Desired Outcome	Incident Examples	Actor Examples	Incident Examples
Cyber criminal	Cyber criminals are hostile by nature with variable skill levels. Cyber criminals may be individuals or organised on a local, national or even international level	Financial gain	• Stealing credit card details or passwords to commit fraud. • Gaining access to and selling personal information for identity theft. • Ransoming a users data for money	• Russian business network • 25 year old unemployed Cowra (NSW) man.[85]	• eBay customer data breach • CryptoLocker malicious software • Alleged breach of 100 or more Australian small business by Romanian cyber criminals.[86]
Issue-motivated group or hacktivist	Seek to disrupt and degrade governments and business to embarrass the target and/or to draw attention to their own cause.[87] The most extreme potential group are cyber terrorists who seek to instil fear in their victims.[88]	Highlight a cause or to gain notoriety	• Defacing or changing the content of websites. • Rending systems or data unavailable to legitimate users to gain media attention.	• Anonymous and LulzSec • Syrian Electronic Army (SEA).[89]	• Anonymous taking Australian Government systems offline to protest internet filtering legislation. • Indonesian hackers targeting Australian Government sites in the wake of the 2013 spying scandal. • Hacking and defacement of US media sites by SEA.[90]
Trusted insider	Employees, outsourcing providers, contractors, consultants with logical or physical access to the targeted ICT system. They can be both non-hostile threat agents (ie distracted or unwitting employees) and hostile ones (ie disgruntled employees).[91]	Unauthorised access to information and intellectual property	• Theft of trade secrets, sensitive plans or business information. • Theft of government classified/ unclassified information.	• Edward Snowden • Private Bradley (now Chelsea) Manning	• US National Security Agency breach. • Leak of US diplomatic cables to Wikileaks.[92]

Malicious Cyber Actor	Description	Desired Outcome	Incident Examples	Actor Examples	Incident Examples
Nation state-supported	Either highly-organised or loosely-affiliated groups of individuals who undertake actions with the tacit support, be that financial or capability support, of a nation state.	Disrupt, deny or degrade access to systems or the information they process	Prevent access to critical infrastructure systems or critical business systems on which a business or government relies, for nuisance or preventing activities not in the attackers' interest.	• Iran's Cyber Army and Ashiyane Digital Security Team allegedly supported by Iran's Islamic Revolutionary Guard Corps • SEA.[93]	
		Highlight a cause or to gain notoriety	• Defacing or changing the content of websites. • Rending systems or data unavailable to legitimate users to gain media attention.	SEA[94]	• Anonymous taking Australian Government systems offline to protest Internet filtering legislation. • Indonesian hackers targeting Australian Government sites in the wake of the 2013 spying scandal. • Hacking and defacement of US media sites by SEA.[95]
Nation state	Directly employed by nation states to progress their political, economic, military or diplomatic interests. They are generally the most sophisticated and well-resourced actors and may have a range of capabilities to undertake espionage or disruption.[96]	Unauthorised access to information and intellectual property	• Theft of trade secrets, sensitive plans or business information.[97] • Theft of government classified/ unclassified information.	No actor claimed responsibility	Alleged breaches and theft of intellectual property, sensitive security information and official communications at: • Lockheed Martin, • Australia's Parliament House, and • Reserve Bank of Australia.[98]
		Disrupt, deny or degrade access to systems or the information they process	Prevent access to critical infrastructure systems or critical business systems on which a business or government relies for nuisance or preventing activities not in the attackers interest.	No actor claimed responsibility	• Stuxnet virus that disrupted Iranian nuclear enrichment, • Attack on Saudi Aramco to prevent oil production, and • The attack on Estonian systems allegedly by Russian hackers.[99]

Notes

1 Department of the Prime Minister and Cabinet, *Strong and Secure: a strategy for Australia's national,* Australian Government: Canberra, 2013, p. III.

2 Department of the Prime Minister and Cabinet, *Strong and Secure,* p. II.

3 Department of the Prime Minister and Cabinet, *Strong and Secure,* p. 40

4 Australian Signals Directorate, *2014 Australian Government Information Security Manual: executive companion*, Australian Government: Canberra, June 2014, p. 4.

5 Josh Rogin, 'NSA Chief: cybercrime constitutes the "greatest transfer of wealth in history"', *Foreign Policy* website, available at <http://thecable.foreignpolicy.com/posts/2012/07/09/nsa_chief_cybercrime_constitutes_the_greatest_transfer_of_wealth_in_history> accessed 31 July 2014.

6 Central Intelligence Agency, 'The World Factbook: world', available at <https://www.cia.gov/library/publications/the-world-factbook/geos/xx.html> accessed 4 September 2014; McAfee, 'The Economic Impact of Cyber Crime and Cyber Espionage', p. 5, available at <http://www.mcafee.com/au/resources/reports/rp-economic-impact-cybercrime.pdf> accessed 21 July 2014.

7 Symantec Corporation, '2013 Norton Report: Australia', p. 1 (noting that the figures are also expressed in terms of purchasing power parity), available at <http://www.symantec.com/content/en/us/about/presskits/b-norton-report-2013-australia.pdf> accessed 21 July 2014.

8 Symantec Corporation, '2013 Norton Report', p. 1.

9 Attorney-General's Department, *Cyber Crime & Security Survey Report 2013,* CERT Australia*:* Canberra, 2014, p. 22.

10 Ponemon Institute, 'Exposing the Cybersecurity Cracks: a global perspective', p. 2, available at <http://www.websense.com/assets/reports/report-ponemon-2014-exposing-cybersecurity-cracks-en.pdf> accessed 25 July 2014.

11 Kaspersky Labs, 'Global Corporate IT Security Risks: 2013', p. 16, available at <http://media.kaspersky.com/en/business-security/Kaspersky_Global_IT_Security_Risks_Survey_report_Eng_final.pdf> accessed 31 July 2014.

12 Australian Bureau of Statistics, '1345.0 - Key Economic Indicators, 2014', available at <http://www.abs.gov.au/AUSSTATS/abs@.nsf/mf/1345.0?opendocument?opendocument> accessed 4 September 2014.

13 National Bank, 'Online Retail Sales Index: in-depth report – July 2014', 3 September 2014, available at <http://business.nab.com.au/online-retail-sales-index-in-depth-report-july-2014-7818/> accessed 10 March 2015.

14 Boston Consulting Group, 'The Internet Economy in the G20: the $4.2 trillion growth opportunity', available at <https://www.bcg.com/documents/file100409.pdf> accessed 4 September 2014.

15 Stewart Baker, Shaun Waterman and George Ivanov, 'In the Crossfire: critical infrastructure in the age of cyber war', p. 4, available at <http://img.en25.com/Web/McAfee/NA_CIP_RPT_REG_2840.pdf> accessed 4 September 2014; Stewart Baker, Natalia Filipiak and Katrina Timlin, 'In the Dark: crucial industries confront cyber attacks', p. 10, available at <http://www.mcafee.com/au/resources/reports/rp-critical-infrastructure-protection.pdf> accessed 4 September 2014.

16 Baker *et al*., 'In the Dark', pp. 10-1.

17 SCADA Systems and Computer Security, 'Industrial Risk Assessment Map', available at <https://www.scadacs.org/iram.html> accessed 4 September 2014.

18 Colin Barker, 'Small companies ignore cyber crime threat, put bigger companies at risk', ZDNet website, available at <http://www.zdnet.com/small-companies-ignore-cyber-crime-threat-put-bigger-companies-at-risk-7000033481/> accessed 11 September 2014.

19 Siobhan Gorman and Shara Tibken, 'RSA forced to replace nearly all of its millions of tokens after security breach', *The Australian*, 7 June 2011. The second-order breach allegedly extended also to include Northrop Grumman and L-3 Communications.

20 Attorney-General's Department, *Australian Cyber Security Strategy 2009*, p. V, available at <http://www.ag.gov.au/RightsAndProtections/CyberSecurity/Documents/AG%20Cyber%20Security%20Strategy%20-%20for%20website.pdf> accessed 20 July 2014.

21 'Rogers: cybersecurity is the "ultimate team sport"', *The Federal Times*, available at <http://www.federaltimes.com/article/20140708/CYBER/307080015/Rogers-Cybersecurity-ultimate-team-sport-> accessed 2 August 2014.

22 Australian Signals Directorate, 'Information Security References', available at <http://www.asd.gov.au/publications/index.htm#tabs-1> accessed 3 August 2014; CERT Australia, 'Advice', available at <https://www.cert.gov.au/advice> accessed 3 August 2014; Australian Government, 'Stay Smart Online', available at <http://www.staysmartonline.gov.au/> accessed 3 August 2014; Australian Federal Police (AFP), 'Cyber Crime: crime prevention', available at <http://www.afp.gov.au/policing/cybercrime/crime-prevention.aspx> accessed 3 August 2014; ThinkUKnow Australia, 'ThinkUKnow', available at <http://www.thinkuknow.org.au/> accessed 3 August 2014; and Australian Communications and Media Authority, 'cyber(smart:)', available at <http://www.cybersmart.gov.au/> accessed 3 August 2014.

23 AFP, 'Cyber Crime'.

24 Australian Signals Directorate, 'CSOC - Cyber Security Operations Centre', available at <http://www.asd.gov.au/infosec/csoc.htm> accessed 3 August 2014; and CERT Australia, 'About us', available at <https://www.cert.gov.au/about> accessed 3 August 2014.

25 Queensland Police, 'E-Crime', available at <http://www.police.qld.gov.au/programs/cscp/eCrime/> accessed 3 August 2014; Victoria Department of Justice, 'Cybercrime', available at <http://www.justice.vic.gov.au/home/safer+communities/crime+prevention/cybercrime> accessed 3 August 2014; NSW Police Force, 'Cyber Security', available at <http://www.police.nsw.gov.au/community_issues/fraud_prevention/cyber_security> accessed 3 August 2014; WA Police, 'Technology Crime', available at <http://www.police.wa.gov.au/Crimetypes/Technologycrime/tabid/1934/Default.aspx> accessed 3 August 2014; and SA Police, 'E-Crime', available <http://www.police.sa.gov.au/sapol/safety_security/ecrime.jsp> accessed 3 August 2014.

26 Department of Education, 'School Education', available at <https://education.gov.au/school-education> accessed 3 August 2014; and Parliamentary Education Office and Australian Government Solicitor, *Australia's Constitution, with Overview and Notes by the Australian Government Solicitor*, Australian Government: Canberra, 2010, pp. vi-vii.

27 Australian Government, 'Stay Smart Online: Internet service providers sign up to icode', available at <http://www.staysmartonline.gov.au/news/news_articles/regular/internet_service_providers_sign_up_to_icode> accessed 3 August 2014.

28 Attorney-General's Department, *Australian Cyber Security Strategy 2009,* pp. 17-9; and Department of Communications, 'Use of INTERPOL list to block child abuse content online', available at <http://www.communications.gov.au/online_safety_and_security/mandatory_filtering_legislation_not_proceeding> accessed 3 August 2014.

29 Australian Government, 'Stay Smart Online'.

30 Optus, 'Broadband Internet Security', available at <http://www.optus.com.au/shop/broadband/extras/internet-security#?tab=one> accessed 3 August 2014; and Telstra, 'Telstra Online Security', available at <http://www.telstra.com.au/connectedhome/enhancements/onlinesecurity/> accessed 3 August 2014.

31 Attorney-General's Department, *Australian Cyber Security Strategy 2009,* p. vi.

32 Attorney-General's Department, *Australian Cyber Security Strategy 2009,* p. 1; and Australian Government, *E-Security National Agenda*, National Office for the Information Economy: Canberra, 2001, p. 1.

33 Attorney-General's Department, *Australian Cyber Security Strategy 2009,* p. vii.

34 CERT Australia, 'CERT Australia: about us', available at <https://www.cert.gov.au/about> accessed 28 August 2014.

35 Department of Communications, *Internet Governance*, available at <http://www.communications.gov.au/digital_economy/internet_governance> accessed 2 August 2014; Department of Communications, *International Telecommunication Union*, available at <http://www.communications.gov.au/international/international_telecommunication_union_and_related_engagement/international_telecommunication_union_itu> accessed 2 August 2014; and Department of Foreign

Affairs and Trade (DFAT), *Australia welcomes UN cyber report*, available at <http://www.dfat.gov.au/media/releases/department/2013/dfat-release-20130813b.html> accessed 2 August 2014.

36 Department of the Prime Minister and Cabinet, *Strong and Secure*, p. 40.

37 Department of the Prime Minister and Cabinet, *Strong and Secure,* p. 40.

38 'Managing Cyber Security in an Increasingly Interconnected World: Assistant Secretary Cyber Security Joe Franzi's address to CeBIT Cyber Security Conference', available at <http://www.asd.gov.au/speeches/20140505_ascs_cebit_cyber_security.htm> accessed 2 August 2014.

39 ASIO, 'Ben Chifley Building', available at <http://www.asio.gov.au/About-ASIO/Ben-Chifley-Building.html> accessed 2 August 2014; and 'Managing Cyber Security in an Increasingly Interconnected World'.

40 'Australian Information Security Association: about AISA', available at <https://www.aisa.org.au/> accessed 20 August 2014; CREST Australia, 'Approved Companies', available at <http://www.crestaustralia.org.au/approved.html> accessed 20 August 2014; and International Information Systems Security Certification Consortium (ISC2), 'ISC2 Member Counts', available at <https://www.isc2.org/member-counts.aspx> accessed 20 August 2014.

41 Australian Communications and Media Authority, 'Australian Internet Security Initiative (AISI)', available at <http://www.acma.gov.au/Industry/Internet/e-Security/Australian-Internet-Security-Initiative/australian-internet-security-initiative> accessed 20 August 2014.

42 National Conference of State Legislatures, 'Security Breach Notification Laws', available at <http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx> accessed 11 October 2014.

43 Australian Signals Directorate, 'Information Security', available at <http://www.asd.gov.au/infosec/index.htm> accessed 20 August 2014; and Australian Signals Directorate, 'Report a Cyber Incident', available at <http://www.asd.gov.au/infosec/reportincident.htm> accessed 20 August 2014.

44 'The Cyber SITREP: Deputy Director Cyber and Information Security Division MAJGEN Steve Day speech to the 3rd Annual Australian Defence Magazine Cyber Security Summit', available at <http://www.asd.gov.au/speeches/20130612_ddcis_cyber_sitrep.htm> accessed 31 July 2014.

45 Stilgherrian, 'Australia Deserves a Whack of the Data Breach Notification Stick', ZDNet website, available at <http://www.zdnet.com/australia-deserves-a-whack-of-the-data-breach-notification-stick-7000032273/> accessed 20 August 2014.

46 See, for example, *ACT Work Health and Safety Act 2011*, available at <http://www.legislation.act.gov.au/a/2011-35/> accessed 16 September 2014.

47 Department of Finance, 'Whole of Australian Government Advertising Arrangement', available at <http://www.finance.gov.au/advertising/> accessed 19 September 2014.

48 Department of Finance, *Campaign Advertising by Australian Government Departments and Agencies: full year report 2012-13*, Australian Government: Canberra, 2013, p. 35.

49 Australian Communications and Media Authority, 'Australian Internet Security Initiative'.

50 Australian Communications and Media Authority, 'Australian Internet Security Initiative'.

51 Australian Signals Directorate, 'ISM – Information Security Manual', available at <http://www.asd.gov.au/infosec/ism/index.htm> accessed 29 August 2014.

52 Simon Hansen, 'The Strategist: cyber wrap', Australian Strategic Policy Institute (ASPI) website, available at <http://www.aspistrategist.org.au/cyber-wrap-39/> accessed 29 August 2014.

53 Australian Government, *Critical Infrastructure Resilience Strategy*, Attorney-General's Department: Canberra, 2010, p. 8.

54 Department of Infrastructure and Regional Development, 'Critical Infrastructure Resilience', available at <http://www.infrastructure.gov.au/transport/security/critical.aspx> accessed 21 August 2014.

55 Department of Finance, 'Whole of Australian Government Advertising Arrangement'.

56 Department of Finance, *Campaign Advertising by Australian Government Departments and Agencies*, p. 35.

57 For example, see Mandiant, 'APT1: Exposing One of China's Cyber Espionage Units', available at <http://www.mandiant.com/> accessed 22 August 2014.

58 Australian Government, 'Trusted Information Sharing Network: welcome to the TISN website', available at <http://www.tisn.gov.au/Pages/default.aspx> accessed 22 August 2014.

59 Australian Government, 'Trusted Information Sharing Network: TISN diagram', available at <http://www.tisn.gov.au/Documents/TISN+Diagram+-+PDF+version.pdf> accessed 22 August 2014.

60 Australian Government, 'Trusted Information Sharing Network: IT security group', available at <http://www.tisn.gov.au/Pages/IT-Security-Group.aspx> accessed 22 August 2014.

61 For example, see Center for Internet Security, 'Multi-state ISAC', available at <http://msisac.cisecurity.org/about/> accessed 22 August 2014.

62 Phillip Thomson, 'Canberra's top secret cyber soldier jobs rush', *The Sydney Morning Herald*, 8 September 2014; and Primrose Riordan, 'In face of cuts, Defence hunts for young cyber army', *The Sydney Morning Herald*, 2 June 2014.

63 National ICT Australia, 'Media Release: cybersecurity – Australia's multi-billion-dollar market opportunity', available at <http://www.nicta.com.au/media/current/cybersecurity_australias_multi-billion-dollar_market_opportunity> accessed 22 July 2014.

64 'Cyber Security Challenge Australia: previous challenges', available at <https://www.cyberchallenge.com.au/cysca-2013.html> accessed 22 August 2014.

65 'Cyber Security Challenge Australia: what is CySCA?', available at <https://www.cyberchallenge.com.au/about.html> accessed 22 August 2014.

66 David Francis, 'Why we need to prepare our kids for cyber-jobs – and cyber-warfare', The Week website, available at <http://theweek.com/article/index/266818/why-we-need-to-prepare-our-kids-for-cyber-jobs-mdash-and-cyber-warfare> accessed 11 September 2014.

67 James Andrew Lewis, *Hidden Arena: cyber competition and conflict in Indo-Pacific Asia*, available at <http://csis.org/files/publication/130307_cyber_Lowy.pdf> accessed 21 July 2014.

68 DFAT, 'About us', available at <http://dfat.gov.au/dept/> accessed 25 August 2014; DFAT, 'Berlin-Canberra Declaration of Intent on a Strategic Partnership', available at <http://www.dfat.gov.au/geo/germany/strategic-partnership.html> accessed 25 August 2014; DFAT, 'Japan Country Brief', available at <http://www.dfat.gov.au/geo/japan/japan_brief.html> accessed 25 August 2014; Tobias Feakin, Jessica Woodall and Peter Jennings, *A shared agenda for the Seoul Conference on Cyberspace South Korea 2013,* Special Report, ASPI: Canberra, October 2013; and UN Office for Disarmament Affairs, 'Fact Sheet: developments in the field of information and telecommunications in the context of international security', available at <http://www.un.org/disarmament/HomePage/factsheet/iob/Information_Security_Fact_Sheet.pdf> accessed 25 August 2014, p. 2

69 Prime Minister of Australia, 'Japan-Australia Summit Meeting', available at <http://www.pm.gov.au/media/2014-04-07/japan-australia-summit-meeting> accessed 2 October 2014; Prime Minister of Australia, 'Joint Communiqué - The President of the Republic of Indonesia and the Prime Minister of Australia, Jakarta', available at <http://www.pm.gov.au/media/2013-09-30/joint-communiqu-president-republic-indonesia-and-prime-minister-australia-jakarta> accessed 2 October 2014; Prime Minister of Australia, 'Joint Statement with Prime Minister Modi, New Delhi, India', available at <http://www.pm.gov.au/media/2014-09-05/joint-statement-prime-minister-modi-new-delhi-india> accessed 2 October 2014; and Prime Minister of Australia, 'Vision Statement for a secure, peaceful and prosperous future between the Republic of Korea and Australia', available at <http://www.pm.gov.au/media/2014-04-08/vision-statement-secure-peaceful-and-prosperous-future-between-republic-korea-and> accessed 2 October 2014.

70 Asia Pacific Computer Emergency Response Team, 'About APCERT: mission statement', available at <http://www.apcert.org/about/mission/index.html> accessed 25 August 2014; and Australian Signals Directorate, 'Partners: UKUSA allies', available at <http://www.asd.gov.au/partners/allies.htm> accessed 25 August 2014.

71 Attorney-General's Department, *Australian Cyber Security Strategy 2009*, p. 22.

72 UN General Assembly, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, available at <http://www.un.org/ga/search/view_doc.asp?symbol=A/68/98> accessed at 25 July 2014.

73 Council of Europe, 'Convention on Cybercrime: chart of signatures and ratifications', available at <http://conventions.coe.int/Treaty/Commun/print/ChercheSig.asp?NT=185&CL=ENG> accessed 26 August

2014; and UN, 'Member States: growth in United Nations membership, 1945-present', available at <http://www.un.org/en/members/growth.shtml> accessed 26 August 2014.

74 Timothy Farnsworth, 'China and Russia Submit Cyber Proposal', Arms Control Today website, available at <https://www.armscontrol.org/act/2011_11/China_and_Russia_Submit_Cyber_Proposal> accessed 26 August 2014.

75 Farnsworth, 'China and Russia Submit Cyber Proposal'; and Tobias Feakin, 'International cyber security: a divided road', ASPI website, available at <http://www.aspistrategist.org.au/international-cyber-security-a-divided-road/> accessed 18 September 2014.

76 Lenore Taylor, 'Ten things to know about foreign policy under Julie Bishop and Tony Abbott', *The Guardian*, available at <http://www.theguardian.com/world/2013/jun/02/foreign-policy-julie-bishop-coalition> accessed 8 September 2014.

77 Mandiant, 'APT1', pp. 39-40.

78 International Cyber Policy Centre, *Cyber Maturity in the Asia–Pacific Region*, ASPI: Canberra, April 2014.

79 International Cyber Policy Centre, *Cyber Maturity In The Asia–Pacific Region*, p. 5.

80 Leon Spencer, 'AFP to embark on international placements in cybercrime fight', ZDNet website, available at <http://www.zdnet.com/afp-to-embark-on-international-placements-in-cybercrime-fight-7000033513/> accessed 11 September 2014.

81 AFP, 'International Liaison', available at <http://www.afp.gov.au/policing/international-liaison.aspx> accessed 26 August 2014.

82 Attorney-General's Department, *National Plan to Combat Cybercrime*, Commonwealth of Australia: Canberra, 2013, pp. 18-9.

83 Attorney-General's Department, 'Fact Sheet – Mutual Assistance Overview', available at <http://www.ag.gov.au/Internationalrelations/Internationalcrimecooperationarrangements/MutualAssistance/Documents/Mutual%20assistance%20overview.pdf> accessed 26 August 2014.

84 Attorney-General's Department, 'Mutual Assistance: Australian requests to foreign countries', available at <http://www.ag.gov.au/Internationalrelations/Internationalcrimecooperationarrangements/MutualAssistance/Pages/Mutualassistancerequeststoforeigncountries.aspx> accessed 26 August 2014.

85 'Media Release: AFP arrests Cowra man after landmark hacking investigation', AFP website, available at <http://www.afp.gov.au/media-centre/news/afp/2011/july/afp-arrests-cowra-man-after-landmark-hacking-investigation.aspx> accessed 30 July 2014; and M.E. Kabay and Bradley Guinen, 'The Russian Cybermafia: RBN & the RBS WorldPay attack', NetworkWorld website, available at <http://www.networkworld.com/article/2201011/malware-cybercrime/the-russian-cybermafia--rbn---the-rbs-worldpay-attack.html> accessed 30 July 2014.

86 Alex Hern, 'Cryptolocker: what you need to know', *The Guardian*, available at <http://www.theguardian.com/technology/2014/jun/03/cryptolocker-what-you-need-to-know> accessed 30 July 2014; Andrea Peterson, 'Hackers steal eBay customer details in massive security breach', *BRW* website, available at <http://www.brw.com.au/p/tech-gadgets/hackers_steal_ebay_customer_details_hnRNXIaAji2dJQzhbcPobP> accessed 30 July 2014; and 'Australia's biggest ever data theft: gang busted over credit card crime', *The Sydney Morning Herald*, 29 November 2012.

87 Australian Signals Directorate, *2014 Australian Government Information Security Manual*, p. 4.

88 Louis Marinos and Andreas Sfakianakis, *ENISA Threat Landscape Responding to the Evolving Threat Environment*, The European Network and Information Security Agency: Heraklion (Crete), 2013, p. 26.

89 Kenneth Geers and Ayed Alqartah, 'Syrian Electronic Army Hacks Major Communications Websites', FireEye website, available at <http://www.fireeye.com/blog/technical/cyber-exploits/2013/07/syrian-electronic-army-hacks-major-communications-websites.html> accessed 30 July 2014; Quinn Norton, 'Anonymous 101: introduction to the Lulz', *Wired Magazine*, available at <http://www.wired.com/2011/11/anonymous-101/all/1> accessed 30 July 2014; and 'A Brief History of the LulzSec Hackers', *FoxNews.com*, available at <http://www.foxnews.com/tech/2011/06/21/brief-history-lulzsec-hackers/> accessed 30 July 2014.

90 Andy Greenberg, 'How The Syrian Electronic Army Hacked Us: a detailed timeline', Forbes website, available at <http://www.forbes.com/sites/andygreenberg/2014/02/20/how-the-syrian-electronic-army-hacked-us-a-detailed-timeline/> accessed 30 July 2014; Asher Moses, 'Operation Titstorm: hackers bring down government websites', *The Sydney Morning Herald*, 10 February 2010; and Will Ockenden, 'Crime Stoppers website hacked, police email addresses published in spying scandal "payback"', *ABC News*, available at

<http://www.abc.net.au/news/2013-11-26/crime-stoppers-site-targeted-by-indonesian-hackers/5116856> accessed 30 July 2014.

91 Marinos and Sfakianakis, *ENISA Threat Landscape Responding to the Evolving Threat Environment*, p. 26.

92 'Edward Snowden: Leaks that exposed US spy programme', British Broadcasting Corporation website, available at <http://www.bbc.com/news/world-us-canada-23123964> accessed 31 July 2014; and 'Bradley Manning sentenced to 35 years' jail for WikiLeaks data breach', *ABC News*, available at <http://www.abc.net.au/news/2013-08-21/soldier-bradley-manning-sentenced-to-35-years-jail/4903854> accessed 31 July 2014.

93 Gabi Siboni and Sami Kronenfeld, 'Iran and Cyberspace Warfare', *Military and Strategic Affairs*, Vol. 4, No. 3, December 2012, pp. 86-91; and Geers and Alqartah, 'Syrian Electronic Army Hacks Major Communications Websites'.

94 Geers and Alqartah, 'Syrian Electronic Army Hacks Major Communications Websites'; Norton, 'Anonymous 101'; and 'A Brief History of the LulzSec Hackers'.

95 Greenberg, 'How The Syrian Electronic Army Hacked Us'; Moses, 'Operation Titstorm'; and Ockenden, 'Crime Stoppers website hacked, police email addresses published in spying scandal "payback"'.

96 Australian Signals Directorate, *2014 Australian Government Information Security Manual*, p. 4; and Marinos and Sfakianakis, *ENISA Threat Landscape Responding to the Evolving Threat Environment*, p. 26.

97 The Australian Signals Directorate estimates approximately 65 per cent of nation state intrusions it responds to have an economic driver: see 'The Cyber SITREP'.

98 'China spies suspected of hacking Julia Gillard's emails', News.com.au website, available at <http://www.news.com.au/technology/federal-ministers-emails-suspected-of-being-hacked/story-e6frfrnr-1226029713668> accessed 29 July 2014; Christopher Joye, 'Cyber-attackers penetrate Reserve Bank networks', *Australian Financial Review*, available at <http://www.afr.com/p/national/cyber_attackers_penetrate_reserve_FEdCLOI50owRMgI0urEYnK> accessed 30 July 2014; and Nathan Hodge and Ian Sherr, 'Lockheed Martin Hit By Security Breach', *The Wall Street Journal*, available at <http://online.wsj.com/news/articles/SB10001424052702303654804576350083016866022> accessed 30 July 2014.

99 Ian Traynor, 'Russia accused of unleashing cyberwar to disable Estonia', *The Guardian*, available at <http://www.theguardian.com/world/2007/may/17/topstories3.russia> accessed 30 July 2014; Josh Halliday, 'Stuxnet worm is aimed to sabotage Iran's nuclear ambition, new research shows', *The Guardian*, available at <http://www.theguardian.com/technology/2010/nov/16/stuxnet-worm-iran-nuclear> accessed 30 July 2014; and Nicole Perlroth, 'In Cyberattack on Saudi Firm, US Sees Iran Firing Back', *New York Times*, available at <http://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html?pagewanted=all&_r=0> accessed 30 July 2014.

Additional reading

(sources not already included in end-notes)

Aiken, Klee, *Cyber Security by Executive Order*, Australian Strategic Policy Institute (ASPI): Canberra, February 2014.

Aiken, Klee and David Lang, 'Governing the Net: from Bondi to Copacabana', ASPI website, available at <http://www.aspistrategist.org.au/governing-the-net-from-bondi-to-copacabana/> accessed 25 July 2014.

Aiken, Klee and David Lang, 'Governing the Net: NETmundial and the status quo', ASPI website, available at <http://www.aspistrategist.org.au/governing-the-net-netmundial-and-the-status-quo/> accessed 25 July 2014.

Arico, Sandra and Vivek Srinivasan, *Enabling Australia's Digital Future: cyber security trends and implications*, CSIRO: Canberra, 2014.

Australian Bureau of Statistics, '8153.0 - Internet Activity, Australia, December 2013', available at <http://www.abs.gov.au/ausstats/abs@.nsf/Lookup/E9B5934F326E48EECA257CB300132152?opendocument> accessed 22 August 2014.

Australian Crime Commission, *Cyber and Technology Enabled Crime*, Australian Crime Commission: Canberra, July 2013.

Australian Curriculum Assessment and Reporting Authority, 'General Capabilities: information and communication technology (ICT)', available at <http://www.australiancurriculum.edu.au/GeneralCapabilities/Pdf/ICT> accessed 22 August 2014.

Australian Federal Police (AFP), 'Cyber Crime', available at <http://www.afp.gov.au/policing/cybercrime.aspx > accessed 3 August 2014.

Australian Government, 'Stay Smart Online', available at <http://www.staysmartonline.gov.au/> accessed 3 August 2014.

Australian Signals Directorate, *Cyber Security Picture 2013*, Australian Signals Directorate: Canberra, June 2014.

Australian Signals Directorate, *2014 Australian Government Information Security Manual: principles*, Australian Signals Directorate: Canberra, June 2014.

Australian Strategic Policy Institute (ASPI), 'Submission to the National Commission of Audit from the Australian Strategic Policy Institute: Submission Two: National Security', available at <https://www.aspi.org.au/media-centre/parliament/parliamentary-submissions/submission-to-the-national-commission-of-audit-submission-two-national-security/ASPI-NCA-National-Security-Submission.pdf> accessed 20 July 2014.

Bailey, Tucker, Andrea Del Miglio and Wolf Richter, 'The rising strategic risks of cyberattacks', *McKinsey Quarterly*, available at <http://www.mckinsey.com/insights/business_technology/the_rising_strategic_risks_of_cyberattacks> accessed 21 July 2014.

Bailey, Tucker, James Kaplan and Chris Rezek, 'Why senior leaders are the front line against cyberattacks', McKinsey website, available at <http://www.mckinsey.com/insights/business_technology/why_senior_leaders_are_the_front_line_against_cyberattacks> accessed 22 July 2014.

Blackburn, John and Gary Waters, *Optimising Australia's Response to the Cyber Challenge*, Kokoda Foundation: Canberra, February 2011.

Center for Strategic and International Studies (CSIS), *Securing Cyberspace for the 44th Presidency*, CSIS: Washington DC, December 2008.

Clemente, Dave, *Compelled to control: conflicting visions of the future of cyberspace*, ASPI: Canberra, October 2013.

Connolly, Chris, Alana Maurushat, David Vaile and Peter van Dijk, *An Overview of International Cyber-Security Awareness Raising and Educational Initiatives*, available at <http://www.acma.gov.au/webwr/_assets/main/lib310665/galexia_report-overview_intnl_cybersecurity_awareness.pdf> accessed 19 July 2014.

Coyne, Allie, 'Govt inquiry backs mandatory data breach notifications', ITNews website, available at <http://www.itnews.com.au/News/389679.govt-inquiry-backs-mandatory-data-breach-notifications.aspx> accessed 25 July 2014.

Danzig, Richard J., *Surviving on a Diet of Poisoned Fruit: reducing the national security risks of America's cyber dependencies*, Center for a New American Security, available at <http://www.cnas.org/surviving-diet-poisoned-fruit#.U9B5cqi-sTw> accessed 24 July 2014.

European Network and Information Security Agency, *National Cyber Security Strategies: practical guide on development and execution*, available at <http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-an-implementation-guide> accessed 21 July 2014.

Executive Office of the President of the United States, *The Comprehensive National Cybersecurity Initiative*, available at <http://www.whitehouse.gov/issues/foreign-policy/cybersecurity/national-initiative> accessed 24 July 2014.

FireEye, 'Advanced Threat Report 2013', available at <https://www2.fireeye.com/advanced-threat-report-2013.html> accessed 21 July 2014.

Gagliordi, Natalie, 'Retailers to share threat data in cybersecurity powwow', ZDNet website, available at <http://www.zdnet.com/retailers-to-share-threat-data-in-cybersecurity-powwow-7000028418/> accessed 25 July 2014.

Goodwin, Christin Flynn and J. Paul Nicholas, 'Developing a National Strategy for Cybersecurity', available at <http://blogs.microsoft.com/on-the-issues/2013/10/04/microsoft-releases-best-practices-for-developing-a-national-strategy-for-cybersecurity/> accessed 19 July 2014.

Government of Canada, *Canada's Cyber Security Strategy: for a stronger and more prosperous Canada*, Government of Canada: Ottawa, 2011.

Government of Japan, *Cyber Security Strategy*, Information Security Policy Council: Tokyo, June 2013.

Government of South Australia, 'Policies, Standards and Guidelines: security', available at <http://www.dpc.sa.gov.au/policies-standards-and-guidelines#Security> accessed 3 August 2014.

Her Majesty's Government, *A Strong Britain in an Age of Uncertainty: the national security strategy*, UK Government: London, October 2010.

Jacques, Jeremiah, 'Russia's Proxy War on Ukraine Becoming Open War', The Trumpet website, available at <http://www.thetrumpet.com/article/11939.32351.0.0/world/military/russias-proxy-war-on-ukraine-becoming-open-war?preview> accessed 31 July 2014.

Jennings, Peter and Tobias Feakin, *The emerging agenda for cybersecurity*, ASPI: Canberra, July 2013.

Kamal, Ahmad, *The Law of Cyber-Space: an invitation to the table of negotiations*, UN Institute of Training and Research: Geneva, October 2005.

Lewis, James Andrew, *Cyber Threat and Response: combating advanced attacks and cyber espionage*, available at <http://csis.org/files/publication/140313_FireEye_WhitePaper_Final.pdf> accessed 21 July 2014.

Lewis, James Andrew, *Liberty, Equality, Connectivity: transatlantic cybersecurity norms*, Center for Strategic and International Studies: Washington DC, February 2014.

Lewis, James Andrew, *Rethinking Cybersecurity – A Comprehensive Approach*, Center for Strategic and International Studies, available at <http://csis.org/files/publication/110920_Japan_speech_2011.pdf> accessed 18 July 2014.

MacGibbon, Alastair, *Cyber security: threats and responses in the information age*, ASPI: Canberra, December 2009.

Ministry of Defence of Estonia, *Cyber Security Strategy*, available at <http://www.kmin.ee/files/kmin/img/files/Kuberjulgeoleku_strateegia_2008-2013_ENG.pdf> accessed 20 July 2014.

Ministry of Foreign Affairs – Republic of Korea, 'Seoul Conference on Cyberspace 2013', available at <http://www.mofa.go.kr/english/visa/images/res/Cy_Eng.pdf> accessed 26 August 2014.

National Institute for Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*, National Institute for Standards and Technology: Gaithersburg, February 2014.

New Zealand Government, *New Zealand's Cyber Security Strategy*, New Zealand Government: Wellington, June 2011.

Organisation for Economic Cooperation and Development, *Cybersecurity Policy Making at a Turning Point: analysing a new generation of national cybersecurity strategies for the Internet economy*, OECD: Paris, 2012.

Ponemon Institute, *Critical Infrastructure: Security Preparedness and Maturity*, available at <http://www.unisys.com/unisys/inc/pdf/misc/14-0316.pdf> accessed 21 July 2014.

Prime Minister of Japan and His Cabinet, *National Security Strategy 17 December 2013 (provisional translation),* Japanese Government: Tokyo, 17 December 2013.

Ranger, Steve, 'From the Cold War to the Code War: UK boosts spending on cyber warfare', ZDNet website, available at <http://www.zdnet.com/from-the-cold-war-to-the-code-war-uk-boosts-spending-on-cyber-warfare-7000031560/> accessed 25 July 2014.

Richards, Kelly, *The Australian Business Assessment of Computer User Security: a national survey*, Australian Institute of Criminology: Canberra, 2012.

Symantec Corporation, *Internet Security Threat Report 2014: Volume 19*, available at <http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v19_21291018.en-us.pdf> accessed 21 July 2014.

'The Coalition's Policy to Enhance Online Safety for Children', available at <http://lpaweb-static.s3.amazonaws.com/Coalition%202013%20Election%20Policy%20-%20Enhance%20Online%20Safety%20for%20Children.pdf> accessed 3 September 2014.

'The Coalition's Policy for E-government and the Digital Economy', available at <http://lpaweb-static.s3.amazonaws.com/Coalition%27s%20Policy%20for%20E-Government%20and%20the%20Digital%20Economy.pdf> accessed 3 September 2014.

The Economist Intelligence Unit, 'Cyber Incident Response: are business leaders ready?', available at <http://www.economistinsights.com/technology-innovation/analysis/cyber-incident-response> accessed 19 July 2014.

The Economist Special Report, 'Cyber Security: Defending the Digital Frontier', *The Economist*, 12-19 July 2014.

The European Commission, *Cybersecurity Strategy of the European Union: an open, safe and secure cyberspace*, available at <http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf> accessed 22 July 2014.

The Whitehouse, *Cyberspace Policy Review: assuring a trusted and resilient information and communications infrastructure*, The White House: Washington DC, 2011.

The Whitehouse, *International Strategy for Cyberspace: prosperity, security, and openness in a networked world*, The White House: Washington DC, May 2011.

The White House, *National Security Strategy*, US Government: Washington DC, May 2010.

Thomas, Rachel Nyswander, *Securing Cyberspace through Public-Private Partnership: a comparative analysis of partnership models*, available at <http://csis.org/files/publication/130819_tech_summary.pdf> accessed 23 July 2014.

UK Government, *The UK Cyber Security Strategy: protecting and promoting the UK in a digital world*, UK Government: London, November 2011.

US Department of State, 'Independent States in the World', available at <http://www.state.gov/s/inr/rls/4250.htm> accessed 26 August 2014.

US Department of State, 'International Cyber Diplomacy: promoting openness, security and prosperity in a networked world', available at <http://www.state.gov/documents/organization/168901.pdf> accessed 24 July 2014.

Verizon, *2014 Data Breach Investigations Report*, available at <http://www.verizonenterprise.com/DBIR/2014/> accessed 21 July 2014.

VICE CHIEF OF THE DEFENCE FORCE

Australian Defence College

Centre for Defence and Strategic Studies

http://www.defence.gov.au/adc/publications/

twitter: @CDSS_

DPS OCT045-14