OPTIMISING AUSTRALIA’S RESPONSE TO THE CYBER CHALLENGE

John Blackburn
and
Gary Waters

The Kokoda Foundation

www.kokodafoundation.org

Researching Australia’s Security Challenges
Australia’s Response to the Cyber Challenge

PREFACE

This publication would not have been possible without the support and assistance of the departments and agencies within the Australian national security community and a broad range of industry representatives. The senior officials and industry leaders who participated in the project were insightful and exceptionally helpful. The Cyber study comprised two colloquiums and two closed workshops held in Canberra between June and August 2010. We would like to thank all of those who contributed in the workshops and the associated interviews and meetings.

The project would not have been possible without the generous support of our sponsors. The Principal sponsor was Accenture. The major sponsors were the Attorney-General’s Department, BAE Systems and Northrop Grumman. We also recognise the support of the Kokoda Foundation sponsors Jacobs and the Department of Defence.

Given the breadth of the Cyber security challenge, this report can only provide a high level overview of the cyber challenges faced by our nation. Readers who wish to discuss and debate aspects are encouraged to do so by preparing either a short commentary or a longer article for the Kokoda Foundation’s professional journal, Security Challenges. For details on how this can be done please visit:

http://www.kokodafoundation.org/journal/New%20Site/author.html

John Blackburn
Gary Waters
EXECUTIVE SUMMARY

The Australian Government’s 2009 Cyber Security Strategy states that cyber security is one of Australia’s top-tier national security priorities. It highlights that Australia’s national security, economic prosperity and social wellbeing are critically dependent upon the availability, integrity and confidentiality of a range of information and communications technologies.

There is a growing threat from state and non-state actors who compromise, steal, change or destroy information and information systems upon which societies depend. This report examines the nature of the cyber challenge confronting Australia and how such a threat can be better addressed. Australia may well have reached a “tipping point” where the current trajectory of cyber responses is being rapidly outpaced by the evolving threat.

In seeking to maintain a secure, resilient and trusted electronic operating environment that supports Australia’s national security and maximises the benefits of the digital economy, the Australian Government has defined cyber security as “Measures relating to the confidentiality, availability and integrity of information that is processed, stored and communicated by electronic or similar means”.

The government’s strategy is well thought out and clearly identifies key near-term initiatives that address the cyber security threat. However, the breadth, scale and growth rate of the threat are such that the current cyber security program is not keeping pace. In fact, the actions taken to date have helped highlight the scale of the problem and underscored that more needs to be done in order to address the challenge.

A complicating issue is that of public awareness. A large part of the Australian population does not comprehend the scale of the growing cyber threat, nor the potential impact of that threat on personal and national wellbeing. That lack of understanding, and therefore commitment to addressing the
threat, is a fundamental weakness in the individual and collective security of Australians.

This report seeks to answer two fundamental questions: are we doing enough to address the growing threat to our national and individual security in the cyber environment, and if not, what do we need to do?

The report concludes that whilst progress in implementing the government’s 2009 Cyber Security Strategy has been laudable, we are not keeping pace with the growing threat and as a result are placing our collective and individual security at risk. What is lacking is a whole-of-nation, government-led integrated long-term National Cyber Strategy and Plan with defined responsibilities, identified priorities and dedicated resources that recognises the scale of the cyber challenge and the need to address that challenge in a more comprehensive manner.

Australia needs to further harmonise the roles and responsibilities of government, industry and the public. While there will be technical challenges in meeting the evolving threat, the greatest challenges will centre on the cultural and organisational changes that will be needed to improve Australia’s security in the cyber environment. Specific conclusions and recommendations include:

- Develop a whole-of-nation, government-led integrated long-term National Cyber Strategy and Cyber Capability Plan (as a subset of the National Security Strategy) with defined responsibilities, identified priorities and dedicated resources.
- Assign the lead to coordinate cyber-related security issues across government to the Office of the National Security Adviser.
- Continue to build on the current cyber programs but with some process and structural change to ensure the cyber threat is understood and cyber vulnerabilities are reduced, a credible counter-attack capability is developed, continuous technology
discovery is pursued, culture change is effected, and alignment with key allies is achieved.

- Accelerate systemic change through a suite of proactive measures such as a proposed National Security Innovation Centre, a virtual Cyber Academy, a Cyber Test Range, and a cyber Cooperative Research Centre (CRC). This will help to normalise cyber as a part of everyday activity.

A key consideration regarding any recommended actions is that of timing - the gap between threat and response capabilities is growing. In the aftermath of the global economic crisis all governments are faced with increasing financial pressures. Projected growth in public and private debt as well as social security and health costs will likely exacerbate these financial pressures in the future. If we do not increase our focus on cyberspace, the threat will grow faster than our response and the cost of addressing the growing threat gap in the future will increase, possibly exponentially. Any delay in taking action may prove unaffordable in the long-term and introduce greater risks.
ACKNOWLEDGEMENTS

The Kokoda Foundation wishes to express its thanks to Accenture, the Attorney-General’s Department, BAE Systems and Northrop Grumman for their generous sponsorship of the project.

The Foundation is also very grateful for the ongoing support of Jacobs Australia and the Department of Defence.
PRINCIPAL SPONSOR PROFILE

Accenture Profile

Accenture Australia Defence are proud to sponsor the Kokoda Foundation’s Cyber Security report. We recognise the tremendous challenges facing Australia in maintaining national security in a time of rapid geopolitical and technological change and the Kokoda Foundation’s important role in stimulating debate on solutions to these challenges. Through our participation in this report and Accenture’s own research, we seek to gain insight into characteristics that help societies and organisations improve security and reduce risks.

Accenture has more than 20 years of experience assisting corporations and governments across the globe deploy security capabilities to defend the enterprise against malicious threats, enable the enterprise to operate innovative business processes and manage risk. By combining our security and technology know-how with industry-specific experience, we help our clients weave cyber resilience into their infrastructure, applications, and core business processes—securing the fabric of their entire organisation.

We address clients’ information security priorities along the full spectrum of activities from risk, strategy to implementation to management. Our experienced group of security professionals is backed by our broad technology, management consulting, and outsourcing teams from across Accenture. We draw on Accenture experts from the relevant industry or capability, such as systems integration or analytics, when their experience will help to measurably improve the outcome. Accenture’s clients include 94 of the Fortune Global 100 and more than three quarters of the Fortune Global 500. With approximately 211,000 people serving clients in more than 120 countries, the company generated net revenues of US$21.6 billion for the fiscal year ended Aug 31, 2010. To read about our Security Services, visit:

www.accenture.com/security.
ABOUT THE AUTHORS

JOHN BLACKBURN, AO

John Blackburn spent thirty-three years in the Royal Australian Air Force, retiring as an Air Vice-Marshal in 2008. John's military experience included test flying at the Aircraft Research and Development Unit and F/A-18 operations with No 77 Squadron which he commanded in 1994/95. His senior Defence roles included the Director General Policy and Plans in Air Force Headquarters, the Director General of Military Strategy and the Head of Strategic Policy for the Australian Department of Defence. In 2004 John was appointed the Commander of the Integrated Area Defence System (IADS) located in Malaysia and Singapore, commanding a multi-national headquarters established to effect the Five Power Defence Arrangements. In 2006, he assumed the role of the Deputy Chief of the Royal Australian Air Force.

John is now a strategic planning consultant to Lockheed Martin, Northrop Grumman and Accenture and a member of the Australian Strategic Policy Institute Council, the NSW Government Defence Industry Advisory Board, the Kokoda Foundation Board and the Williams Foundation Board.

GARY WATERS

Dr Gary Waters spent thirty-three years in the Royal Australian Air Force, retiring as an Air Commodore in 2002. He then spent three years as a senior public servant in Defence before joining Jacobs Australia as Head of Strategy.

He has written twelve books on doctrine, strategy and historical aspects associated with the use of military force. His latest two books are ‘Firepower to Win’ (with Air Vice-Marshal Al Titheridge and Professor Ross Babbage, 2007), and ‘Australia and Cyber Warfare’ (with Professor Des Ball and Ian Dudgeon, 2008).
He is a Fellow of the Royal Melbourne Institute of Technology (graduating with majors in accounting and economics); an Associate of the Australian Society of CPAs; a graduate of the United Kingdom’s Royal Air Force Staff College; a graduate of the University of New South Wales, with an MA (Hons) in history; a graduate of the Australian Institute of Company Directors; and a graduate of the Australian National University with a PhD in political science and international relations.

He has been a Fellow of the Australian Institute of Company Directors and a Vice President of the United Services Institute, and Inaugural Board Member and Treasurer of the Kokoda Foundation.
## CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Preface</td>
<td>i</td>
</tr>
<tr>
<td>Executive Summary</td>
<td>ii</td>
</tr>
<tr>
<td>Acknowledgements</td>
<td>v</td>
</tr>
<tr>
<td>Principal Sponsor Profile</td>
<td>vii</td>
</tr>
<tr>
<td>About the Authors</td>
<td>viii</td>
</tr>
<tr>
<td>Introduction</td>
<td>1</td>
</tr>
<tr>
<td>Background and Context</td>
<td>3</td>
</tr>
<tr>
<td>The Nature of the Cyber Challenge</td>
<td>8</td>
</tr>
<tr>
<td>Responding to the Cyber Challenge</td>
<td>13</td>
</tr>
<tr>
<td>Government’s Roles and Responsibilities</td>
<td>14</td>
</tr>
<tr>
<td>Industry’s Roles and Responsibilities</td>
<td>34</td>
</tr>
<tr>
<td>People, Culture and Workforce</td>
<td>36</td>
</tr>
<tr>
<td>The Need for a National Cyber Strategy and Framework</td>
<td>37</td>
</tr>
<tr>
<td>Conclusions</td>
<td>48</td>
</tr>
<tr>
<td>Annex A: Defence Signals Directorate’s Top Thirty-Five Mitigation Strategies</td>
<td>50</td>
</tr>
<tr>
<td>Annex B: Recommended Actions</td>
<td>54</td>
</tr>
<tr>
<td>Annex C: Measures of Success</td>
<td>62</td>
</tr>
<tr>
<td>About the Kokoda Foundation</td>
<td>66</td>
</tr>
</tbody>
</table>
OPTIMISING AUSTRALIA’S RESPONSE TO THE CYBER CHALLENGE

INTRODUCTION

The Australian Government’s 2009 Cyber Security Strategy states that cyber security is one of Australia’s top-tier national security priorities. It highlights that Australia’s national security, economic prosperity and social wellbeing are critically dependent upon the availability, integrity and confidentiality of a range of information and communications technologies. Unfortunately there is a growing threat from state and non-state actors who compromise, steal, change or destroy information and information systems upon which societies depend.

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’.1 The Government defines cyber security as ‘Measures relating to the confidentiality, availability and integrity of information that is processed, stored and communicated by electronic or similar means’.2

The government’s Cyber Security Strategy is well thought out and clearly identifies key near-term initiatives that address the cyber security threat as it was in 2009; however, the accelerating pace of change and evolving nature of the threat suggest that it should be reviewed in 2011. There still remains a large part of the Australian population that does not comprehend the scale of the growing cyber threat, or the potential impact of that threat on personal and national wellbeing. Some choose to believe that the threat is unlikely to

---

2 Cyber Security Strategy, p.5.
target them individually and therefore not worthy of concern. Others are sceptical, remembering the publicity surrounding the ‘Y2K’ program and the subsequent conclusion that the threat had been overplayed. The lack of understanding and therefore broad commitment to addressing the threat is a fundamental weakness in the individual and collective security of Australians.

The Kokoda Foundation embarked on a study of the cyber challenge faced by Australia for two reasons. First, the government’s identification of cyber security as a national security priority; and second, because of concerns that whilst the actions taken by government and some segments of industry are highly laudable, the breadth, scale and growth rate of the threat are such that the current cyber security program is simply not sufficient.

In order to explore these issues, a series of colloquiums, workshops and interviews were conducted with representatives of government departments, industry and other relevant parties. Former US Government officials as well as US and UK industry representatives participated in the colloquiums, along with a large representation of Australians.

This report examines the nature of the cyber challenge confronting Australia and how such a threat is being and can be better addressed. It reviews how government, industry and the public are responding to the threat both individually and collectively from both a domestic and international perspective. It seeks to answer two fundamental questions:

- are we doing enough to address the growing threat to our national and individual security in the cyber environment; and
- if not, what do we need to do?
BACKGROUND AND CONTEXT

The Attorney-General’s Department (AGD) chairs the Cyber Security Policy and Coordination (CSPC) Committee. It also takes a leadership role in advancing business-government partnerships, including national Computer Emergency Response Team (CERT) arrangements, and in providing cyber security guidance to owners and operators of critical infrastructure and other businesses of national interest.

Systems of national interest include the traditional critical infrastructures such as electricity grids, water storage and distribution, aviation and maritime transport, and telecommunications networks. They also include systems of high economic value such as those that support electronic transactions, hold sensitive intellectual property such as biotechnology patents or other commercial data associated with major international trade negotiations. In essence, systems of national interest are those systems which, if rendered unavailable or otherwise compromised could result in significant impacts on Australia’s economic prosperity, international competitiveness, public safety, social wellbeing or national defence and security.

Control systems, which include supervisory control and data acquisition (SCADA) systems, are devices and networks used to electronically control mechanical processes such as water valves, electricity generation and transmission. The Australian Government is working with control systems owners

---

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

and operators to help them secure their systems. Under the auspices of the Trusted Information Sharing Network for Critical Infrastructure Protection (TISN), the Australian Government has:5

- Provided guidance and advice to TISN member organisations on control systems security in the form of advisories and alerts on specific vulnerabilities and threats to control systems and networks.
- Established a SCADA Community of Interest to provide a forum to raise the awareness of security for control systems practitioners from critical infrastructure sectors, vendors, consultants and researchers.
- Supported control systems practitioners participating in world’s best practice training in advanced control systems cyber security conducted in the United States.

TISN was launched at the National Summit on Critical Infrastructure Protection on 2 April 2003. It provided an overarching statement of principles for critical infrastructure protection in Australia, outlined the major tasks and assigned the necessary responsibilities across Government, the owners and operators of infrastructure, their representative bodies, professional associations, regulators and standards setting institutions. The TISN allows owners and operators of critical infrastructure to share information on issues related to the protection of critical infrastructure within and between their respective industry sectors. These issues include business continuity, consequence management, information system vulnerabilities and attacks, e-crime and the protection of key sites.

CERT Australia was established in 2010 to offer a single coordination point within the Australian Government for the provision of information and advice and thus provide a more

integrated, holistic approach to cyber security across the Australian community. CERT Australia.\(^6\)

- Provides Australians with access to information on cyber threats, vulnerabilities in their systems and information on how to better protect themselves.
- Promotes greater shared understanding between government and business of the nature and scale of cyber threats and vulnerabilities within Australia’s private sector networks and how these can be mitigated.
- Provides targeted advice and assistance to enable the owners and operators of critical infrastructure and other systems of national interest to defend their systems from sophisticated electronic attacks, working in close collaboration with intelligence and law enforcement agencies, via the Cyber Security Operations Centre (CSOC) within the Defence Signals Directorate (DSD).
- Provides a single Australian point of contact in the expanding global community of national CERTs to support more effective international cooperation.

The Australian Government, through CERT Australia, now operates trusted information exchanges with the owners and operators of control systems. This enables government and business to share sensitive and detailed technical security information, thereby building a greater understanding of the control systems environment and its threats. However, as subsequent discussion in this report shows, greater collaboration, transparency and dialogue is needed with industry.

Established in the DSD as an initiative of the Australian Government’s Defence White Paper 2009, the CSOC provides the Australian Government with all-source cyber situational awareness and an enhanced ability to facilitate operational

\(^6\) More information on CERT Australia can be found at www.cert.gov.au. See also Cyber Security Strategy, p.9.
responses to cyber security events of national importance. The CSOC’s core functions include:7

- Providing comprehensive understanding of the cyber threat and the security status of government networks and networks of national importance.
- Identifying and analysing sophisticated cyber attacks and providing government with response options.
- Assisting responses to cyber events across:
  - government, and
  - critical private sector systems and infrastructure in conjunction with CERT Australia.

In detecting and defeating sophisticated cyber threats, the CSOC is staffed by skilled experts from a number of Australian Government agencies. The CSOC draws on an array of sources in the intelligence and security, law enforcement, national CERT and industry communities to provide a comprehensive picture of threats to Australian information and systems. The CSOC coordinates cyber event responses by government agencies and works in collaboration with overseas partners. It also works closely with DSD’s Cyber and Information Security Division.

The Department of the Prime Minister and Cabinet (PM&C) established a National Security Chief Information Officer (NSCIO) position within the Office of the National Security Adviser in 2009 to realise the vision of a secure, coordinated and effective national security community. The work of the NSCIO includes harmonising the broad policy, governance and legislative arrangements currently in place to improve interoperability and collaboration, and to provide oversight of the national security information management environment. One of the CIO’s first tasks was to develop and

---

7 More information on the CSOC can be found at www.dsd.gov.au. See also Cyber Security Strategy, p.9.
promulgate the national security information environment Roadmap for 2020.

The Roadmap involves a staged process over ten years to address policy and technical enhancements in cyberspace. The six stages of the Roadmap include,\(^8\)

- Stage 1 - reforming governance arrangements; and raising awareness of information-sharing barriers.
- Stage 2 – enhancing the ability for classified systems to communicate with each other; standardising policies and agreeing technical standards for federal government systems; and establishing a common security classification terminology across federal systems.
- Stage 3 – ensuring clear, consistent and authoritative guidance for security policies; achieving mutual recognition of personal security clearances; and establishing common standards for metadata.
- Stage 4 – exploring opportunities for cross-domain sharing; and enhancing the ability to collaborate and share information at the highly classified level across the national security community.
- Stage 5 – developing a federation of networks to realise the business benefits of improved sharing, data discovery, shared tools, services and licensing arrangements; and ensuring that the federation of networks can support the rapid establishment and operation of Task Forces to support Government’s requirements.
- Stage 6 - examining emerging technologies that can display multiple security domains securely on a single screen.

In late 2010, PM&C also assigned the lead for Cyber Policy Coordination to the NSCIO within the office of the National Security Adviser.

THE NATURE OF THE CYBER CHALLENGE

In this report the authors conceive of cyberspace as the electronic information environment through which much of a nation’s society functions. It is the primary enabler for Australia’s increasing commerce and economic vibrancy, its societal well-being, and its supporting critical infrastructure. There is some argument about whether or not cyberspace is a ‘domain’. There is a qualitative difference between cyberspace and the physical domains such as space, air, land and maritime. Whilst some may claim that such a model will lead to the militarisation of cyberspace, it can help to think of it as one would of a physical domain when considering how to operate within it and how to secure it.

Security of cyberspace is complicated because it involves the increasing dependence on information networks that, in turn, introduce vulnerabilities and create opportunities to be exploited by criminals, adversaries and others. This challenge is further complicated by the lack of national boundaries; i.e., cyberspace is global. It is also worthwhile to remember that the Internet was originally designed to facilitate rapid transfer of large amounts of information between a limited number of nodes that were known to each other and that were trusted, in order to support research activities. The way the Internet was designed, therefore, favours the intruder whilst complicating the task of the defender.

Much of what is referred to in public or in submissions to Parliamentary Committees as a cyber issue is a social policy issue and not a cyber security issue per se. For example, cyber safety attracts much attention; while it is laudable that Parliament has devoted attention to protecting children and content online, it is essential that the wider question of cyber
security and cyberspace be addressed more fundamentally and, in some instances, less emotively.

It is worthwhile to note that in just a few years information technology has transitioned from being a ‘support function’ to a strategic element of power in its own right; the front lines of national security have been re-defined. The threat posed by cyber extends far beyond military operations; it extends to the very heart of the national economy and its underpinning society. The rapid growth and evolutionary nature of the cyber threat has meant that responses have largely been developed from the bottom up and have been near-term focused, which has meant that government and business have pursued reactive protection paths that have been focused on their respective organisational perspectives with little consideration for alignment or the need to be more proactive.

Whilst the scale of the future threat is difficult to quantify, a useful assessment can be derived from the current scale and cost of the cyber threat and the advice from experts in this field that the growth rate of the threat is such that the current cyber security program in Australia is not keeping pace with it. US President Obama has been quoted as saying that the cost of cyber crime was more than US$8 billion in 2007 and 2008 combined, while the cost of cyber espionage and the theft of intellectual property has risen to around US$ 1 trillion in the past year. Australia’s Cyber Security Strategy cited research that indicated Australia had the fifth highest level of malware infections worldwide in 2008. Harder to quantify is the impact on national and personal security resulting from cyber intrusions.

Reports of such intrusions show that the threat to government, business and individual’s information systems continues to rise at an unmanageable pace. For example, the rise in the type and versatility of malicious and unwanted software detection rates is significant; data released by the McAfee Laboratories show an approximate doubling in the number of malware signatures detected over the last financial year. The McAfee library had in excess of 40,000,000
signatures in their database as of June 2010. These types of threats are the most insidious to the home and small business sectors as these users are less likely to have the necessary patching and anti-virus systems and information assurance measures in place. Threats such as these create cost for business and government as customers experience fraud, the costs of which must be absorbed by businesses themselves. Compromised systems are also utilised as a ‘weapon’ which can, in turn, be used to damage other businesses or government services.

A commonly held view is that the scale of the current and projected cyber threat is of a level to warrant increased focus and attention as a matter of national priority, given the potential impact on Australia’s economic and social wellbeing. A particular focus needs to be placed on the emerging threat posed by specific targeted intrusions designed to exfiltrate specific information or cause specific damage and disruption to national security. This type of malware can be delivered to a specific individual who holds information of either commercial or intelligence value. Defence against such malware requires significantly more sophistication in the information security community and greater public awareness than currently exists.

The following construct is used to explain the nature of Computer Network Operations (CNO) and to distinguish its three forms:

- Computer Network Attack (CNA), which involves actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves;
- Computer Network Exploitation (CNE), which includes enabling actions and intelligence collection through computer networks that exploit data gathered from targeted information systems or networks; and
- Computer Network Defence (CND), which includes measures to protect one’s own computer networks
and systems against CNA and CNE. CND includes actions taken to protect, monitor, analyse, detect, and respond to unauthorised activity.

While cyber intrusions can take a number of forms, they essentially entail stealing information (exploitation) or damaging information or systems (attack). The key threats in the cyber domain include:

- individual hackers and vandals;
- cyber ‘hacktivists’ (including politically-motivated groups);
- cyber criminals, ranging from smart individuals to sophisticated organised crime groups; and
- the intelligence and security agencies of nation states that might carry out cyber espionage (targeting information held in Government and corporate networks) or cyber warfare (warlike conflict that primarily involves information technology means).

While terrorists have the potential to exploit cyber vulnerabilities, they do not as yet appear to have embraced cyber as a means of terrorising citizens; rather, they have used cyberspace to support their operations in terms of funding, recruiting and communicating.

The initial challenge, therefore, is to understand the intent and capability of these various threat actors.

Defensive measures that may be used to deal with all forms of cyber threat include information assurance, which is the responsibility of each individual citizen and company, not just government, as well as measures under private and criminal law. Australia must protect its own networks and, through its legislation, ensure that any existing gaps in Internet law are closed where feasible, while cooperating with other nations to establish agreed international norms and behaviours.

Information assurance must be complemented by critical infrastructure protection, which requires a close partnership
between government and industry as well as intense cooperation with other nations. The real challenge for the future will be in integrating national cyber defence to ensure the full spectrum of threat actors is well-understood and comprehensively addressed – from cyber crime to cyber espionage to an act of war.

Australian governments (federal and state) and businesses can adopt a defence-in-depth approach against cyber intrusions, noting that both the information and the systems must be protected. This would include:

- Static defence, such as anti-virus software, patches, and making oneself as difficult a target as possible. The Defence Signals Directorate has published its top 35 mitigation strategies, which are summarised at Annex A.

- Situational awareness and active deception, which demands sophisticated technology using anomaly detection to detect threats and vulnerabilities in real-time.

- Cyber intelligence, which involves ‘getting over the horizon’ in detecting a threat, and leverages off capabilities at the various layers of the Open Systems Interconnection (OSI) model – such as the physical layer, network layer, data layer, transport layer, applications layer, and so on; use of honey pots (traps to detect or counteract attempts at unauthorised use of information or information systems); and reconnaissance and surveillance of the broader Internet.

- Dynamic cyber defence, which demands a sophisticated detection capability and dynamic re-configuration of systems (such as changing Internet Protocol addresses and ports) to respond to threats.

- Knowledge of where the adversary is storing information and accessing that information (this often
involves a third party) or stopping the adversary from using that third party.

- Protecting critical information from social engineering (manipulating people into divulging information) and the insider threat (malicious activity carried out by employees).

Finally, it is important for the government to determine a declaratory policy on how it will respond to attacks. However, the challenge in developing a coherent declaratory policy is deciding at what threshold something can be considered to be an attack. Determining the threshold between espionage or theft and an outright attack is not easy. The term ‘attack’ is used here in accordance with the earlier definition; in other words, an attack at the nation-state level aimed at disruption or destruction.

**RESPONDING TO THE CYBER CHALLENGE**

Threats of a major magnitude in the physical world have been effectively dealt with in the past but they have demanded focus, commitment, resources and sustained attention. The threat emerging in cyberspace is very significant but difficult to conceptualise; the scale and consequence of the cyber threat is such that Australia’s economic and social wellbeing is at risk if the threat is not addressed systematically. The cyber security challenge is complex; it demands a systems-level response to ensure that all the activities of affected parties\(^9\) can be complementary, mutually reinforcing, proportionate and cost-effective. The likelihood and consequences of the cyber threat require a level of national commitment not seen outside of war; it is a ‘whole-of-nation’ undertaking that reaches from government down to the individual. Indeed, cyber security and cyber safety for Australians will only improve as the practice becomes a societal norm; much in the same way as seatbelts

\(^9\) Federal and State/Territory governments, public sector agencies, private sector companies, and individuals.
and the use of airbags have come to be accepted as fundamental to car safety.

In order to review how the threat can be addressed it was found useful to disaggregate the cyber issue into digestible pieces. The study broadly examined the roles, responsibilities and interactions in three layers: Government, Industry and Public and then how those layers were segmented into areas of responsibility, from the individual through to the State and in turn to the international system, before identifying additional measures necessary to improve Australia’s security response to the threat.

GOVERNMENT’S ROLES AND RESPONSIBILITIES

The Australian Government’s 2009 Cyber Security Strategy articulates the threats and challenges and provides a framework for engagement with industry, the public and across government departments (including the states and territories) with respect to cyber security, which is only one aspect of the cyber spectrum. Government must now provide a similarly cohesive and coordinated response that captures the entirety of the cyber spectrum - the nation cannot afford an uncoordinated and disaggregated policy interface between the public, industry, the states and territories, and international partners. Such an integrated approach would help address the sometimes blurred responsibilities across agencies for various cyber functions and clarify just what constitutes the scope of cyber security.

As mentioned earlier, the Attorney-General’s Department chairs the CSPC Committee and has recently stood up CERT Australia. The focus is very much on promoting security and resilience in infrastructure, networks, products and services, as well as on developing an effective legal framework and enforcement capabilities, promoting the development of a skilled cyber security workforce, and educating Australians on how to protect themselves online.
Current challenges being addressed by the AGD revolve around improving awareness and making cyber protection easier, more effective and seamless. The AGD is focussing on three Industry groups in its efforts to improve cyber security:

- Internet Service Providers (ISPs), banks, and web-hosting companies;
- systems of national interest that are subject to cyber espionage (whilst initially focussed on the 200+ critical infrastructure companies and around 100 defence contractors, this group has grown to more than 460 companies as industry sectors such as mining were included); and
- SCADA systems that have underlying vulnerabilities that could compromise critical infrastructure (e.g., the communications and control systems sectors).

Whilst vulnerabilities of critical infrastructure and SCADA systems are receiving attention, consideration should also be given to mandating progressive changes to such systems as they are upgraded or replaced. For example, significant improvements in system protection could be achieved by:

- disconnecting the power grid and any control system transporting people, managing gas and petrol production or controlling the flow of water from the wider Internet\(^\text{10}\);
- mandating credentials for digital identities\(^\text{11}\) and mandating cyber security standards for companies commensurate with their size or involvement with critical infrastructure; and
- improving capabilities for monitoring and forensic analysis in order that compromises can be rapidly detected and attributed.

\(^{10}\) While such an action would simplify the problem space, it is recognised that this would be a very expensive and disruptive option to implement and that the source of funding to effect such a change would be problematic.

\(^{11}\) If all external interactions needed to be authenticated, it would reduce the potential exfiltration paths as well as potential command and control paths.
The linkages with the Small to Medium Enterprises (SMEs) and home computer users are largely managed through the Department of Broadband, Communications and the Digital Economy (DBCDE). The department has instituted an awareness-raising campaign in partnership with community and industry groups and other government agencies. National Cyber Security Awareness Week caps off that campaign each year. The Australian Federal Police (AFP) provides a response capability and a specialised investigative capacity in relation to complex technology-enabled crime. Stronger links across these three agencies - AGD, DBCDE and AFP - would seem warranted to enable improved awareness and protection across the entire community, and to ensure that individual messages are consistent with and supportive of one another.

From an operational perspective, the four key agencies within the CSOC should form the nucleus of the Government’s response to the cyber threat. These agencies are DSD, AGD (CERT Australia), the AFP and the Australian Security Intelligence Organisation (ASIO). Tighter integration of the capabilities of each, and the synergies that would accrue, need to be pursued.

Whilst the Australian Government is addressing the cyber security of industry, further development is needed in terms of the rights of an individual company to take action against a threat source. For example, the extent to which self-defence against a criminal threat is covered under the self-defence provisions of the criminal code has not been tested in a court of law. Companies acting in self-defence and using measures that could be construed as exploitation or attack would be acting illegally under a number of Commonwealth and State and Territory laws. Increased dialogue and clearer legal guidance in this area is needed to ensure that self defence actions are not illegal and potentially damaging to Australia’s national interests where such activities result in collateral damage to other nations.

The Government’s responsibilities for cyber protection of individuals are even more problematic. The Government
would have difficulty in building a direct relationship with every individual; hence it must reach out through the ISPs and other third parties that have face-to-face dealings with consumers. An emerging option would be to define a more significant role for agencies such as Centrelink in respect of the direct relationship with individuals. The impending integration of government data systems of agencies such as Centrelink and Medicare and the planned migration to provision of services to primarily online, provide the opportunity for Government to build a direct online relationship with the vast majority of Australian citizens who will access these online services. Through targeted education programs, the Government has the opportunity to shape the behaviours of individuals accessing services online and thus improve security within the broader cyber environment.

Introduction of the National Broadband Network (NBN) could provide a tipping point in terms of new and tougher regulation. However, it will be the retail service providers who will be expected to provide security not the NBN backbone. It will be important for NBN Co to ensure security standards are adequate and to build strong relationships with industry associations, the Internet Industry Association and the Internet Society of Australia, and not just with government. At this stage, NBN Co has not articulated its approach to ensuring or improving cyber security. The rollout of the NBN offers a significant opportunity to engage the public to better understand the vulnerabilities that exist and that could be exploited through the significantly increased bandwidth that will be made available, and in turn the responsibilities of individuals as well as the ISPs to take appropriate security measures. This opportunity must be grasped by all relevant parties.

While the code of conduct for ISPs is a good start, it will do little to improve end-point control at a user’s desktop. End-point control assumes that each device (end-point) is responsible for its own security, or to put it another way, end-point security places the onus of security on the device itself.
Australia’s Response to the Cyber Challenge

Only consistent application of security tools and monitoring of the security status of end-users by ISPs will achieve this.

**Coordination across Government**

Cohesive coordination across government is an essential precondition to addressing the growing cyber threat. Whilst the Office of the National Security Adviser (NSA) is engaging with agencies across government, the scope of its role and responsibilities could be more clearly defined. Furthermore, greater clarity of roles and responsibilities across agencies would improve coordination and response. One potential model could see the Department of Prime Minister and Cabinet (PM&C), through the NSA Office, lead the high-level coordination and engagement where a cyber event involves cross-sector or cross-jurisdictional boundaries. The operational response would be coordinated by the Cyber Security Operations Centre.

Figure 1 illustrates this model for improved cross-government coordination, led by PM&C (NSA Office), with component leads being taken by relevant agencies under a central guiding framework, underpinned by the outcomes sought in the cyber environment. At the time of publication, this depiction is reflective of current thinking within Government regarding whole-of-Government coordination. For example:

- fair trading and consumer protection led by Treasury but also involving the Australian Competition and Consumer Commission (ACCC);
- fraud, crime and safety led by AGD, but also involving DBCDE and the AFP;
- security and resilience (in government and with industry) led by the AGD; and
- cyber operations as part of cyber warfare led by the Defence Department.
Figure 1: Cross-Government Coordination View

The model is simplistic in that the responsibility boundaries are not as clearly delineated as is suggested by the illustration. Moreover, departments such as Centrelink do not feature, yet their plans to transition to online service delivery programs will result in significant changes to how individuals access support services. This will result in a greater level of exposure to cyber threats as individuals increasingly access online services. Furthermore, the Defence Signals Directorate is responsible for more than supporting Defence and the Australian Defence Force on information security matters; indeed, it is responsible for providing information security advice and assistance to all federal and state government agencies as well as assisting other government agencies to support industry.

Analysis of this model leads to the following conclusion: a critical issue in cross-government coordination is the need for a central guiding framework. Whilst the Cyber Security Strategy provides a coherent near-term strategy and goals, there is no clear guiding framework or implementation plan that unites departments and agencies under a coordinated
plan that addresses whole-of-nation aspects. There is a need for a mid- to long-term strategy and associated guidance and plans to provide greater coherence in the Government’s approach to cyber security for the entire nation. This issue is discussed further, later in this report.

There is also a need for a clearly defined cyber incident response process that indicates who has responsibility, who has accountability, who should be consulted, and who should be informed. As mentioned earlier, the CSOC and its core contributing agencies must be at the epicentre of any operational-level response.

**So why not a Cyber Czar?**

The United States has appointed a lead for cyber security and is creating a bureaucracy focussed on cyber security. However, such a move would be counterproductive for Australia. A key goal should be to normalise cyber security as just another element of national security. If this goal was achieved in say the next decade, then cyber security would ideally be integrated into all national security functions. The preferred method of addressing the security challenge posed by cyberspace is to provide an increased focus on cyber security but to affect it through an *existing* structure such as the NSA Office which would be best placed to integrate cyber across the broader national security functions. Of note, the recent establishment of the Cyber Policy Coordinator in PM&C is a solid step in this direction.

**States and Territories Coordination**

While much of the discussion to date focuses on what federal agencies need to know and do, the relationship with other jurisdictions is vital. It is crucial that the states and territories are engaged to ensure that the whole-of-nation threat picture can be fully understood. This is especially so with law enforcement agencies who are the first point of contact for the public in the instance of fraud or online crime and exploitation. Furthermore, the jurisdictional responsibilities will be difficult to determine given the difficulty in attributing the
source of an attack; federal agencies need to better understand the challenges that their state and territory partners face and to work with them in deriving solutions. The high-level start point for this should be through the Council of Australian Governments (COAG). A good foundation has been provided by the establishment of the National Cyber Crime Working Group (NCWG) following a decision of the Standing Committee of Attorneys-General in May 2010 to review existing arrangements aimed at combating cyber crime and providing advice on how they could be improved. The NCWG is comprised of representatives from Commonwealth, State and Territory police and justice agencies as well as the Australian Crime Commission (ACC) and CrimTrac. In addition, the Australia New Zealand Policing Advisory Agency e-Crime Committee (AeCC) is responsible for facilitating effective investigation of e-crime across jurisdictions and sharing of technical information and specialist knowledge.

**Government Focus and Funding Levels**

Much of what Government has achieved in recent years is highly laudable but a critical issue is one of capacity to scale up. The lack of priority and resourcing has occurred mainly because cyber security is competing rather poorly against other issues for the attention of politicians and company boards. Many of the cyber issues raised in Parliament are in reality social policy issues and involve problems around human interaction and behaviour. They should be addressed as such rather than divert attention away from the underlying systemic cyber security issues. Similarly, there is a need to improve awareness at senior levels of government bureaucracy (federal and state). An option that could be utilised would be to engage institutions like the Australian Institute of Company Directors and the Risk Management Institution of Australasia. For example, a module on cyber security responsibilities could be included in courses run by such organisations. Furthermore, the nascent National Security College could support increased understanding through its evolving courses.
Australia’s Response to the Cyber Challenge

The lack of a central guiding framework is also impacting the funding of cyber security across government departments and agencies. For example, whilst funding for the Defence CSOC is substantial, the AGD CERT function is funded in the order of A$3M per annum. This funding level appears adequate to establish the CERT but will clearly need to be increased significantly as the CERT function grows in response to the increasing demand for its services and as industry provides greater access to the CERT. The CERT will soon find itself overwhelmed with data that it does not have the tools nor staff to analyse and process into actionable information.

It is vital to determine just what the baseline investment should be as a part of a national security capability plan in order to give some certainty to those departments responsible for improving cyber security and awareness. An example of national commitment to cyber security is the UK Government’s announcement of a £650M cyber security initiative (A$1.04B) as a part of its 2010 Strategic Defence and Security Review, despite significant budget cuts being imposed across the UK Government.

CSOC funding and capabilities should be leveraged to the fullest extent possible by those agencies with embedded staff in the CSOC – such as CERT Australia, ASIO and the AFP. These agencies will be less susceptible to being flooded with data and requests if they are able to exploit the synergies of being located together with the CSOC.

A secondary, but nonetheless significant issue is the funding of cyber security research and development. Departments and agencies outside of Defence do not have dedicated research funds to apply to cyber security. Consequently, bids for cyber research, including under the CRC program, compete with non-cyber programs in the absence of an endorsed cyber research strategy. The security threats Australia faces in the cyber domain need to be addressed with a coherent integrated and funded research program in advance of the threat and not just in reaction to it.
In addition to pure research funding, there appears to be a strong case for the establishment of appropriate tools and test capabilities. For example, a SCADA test bed would appear to be a much-needed capability, particularly if developed as a part of a national cyber test range.

**Government Interaction with the Public**

Whilst there is good work underway in consumer protection and online safety, it can still be confusing and confronting for the public to know where to go for assistance when faced with cyber crime, fraud or other issues. As the Government endeavours to make the cyber environment more secure, it must also raise the public’s awareness of what threats exist and how, as individuals, they can participate in such a way that is both safe and to their benefit, as well as to the nation’s benefit. While it is difficult to change human behaviour, and there will always be a percentage of people who do not report cyber incidents, Government does need to deepen its engagement with the public about cyber threats. The first steps in public awareness have been taken and while Fraud Week, Privacy Week, Cyber Security Awareness Week and others are all effective, greater effect could be obtained through closer coordination of the messages behind such events.

One useful initiative has been the Australian Communications and Media Authority’s (ACMA’s) Australian Internet Security Initiative (AISI) to help address the emerging problem of compromised computers. The AISI collects data from various sources on computers exhibiting ‘botnet’ behaviour on the Australian Internet. Using this data, ACMA provides daily reports to ISPs identifying IP addresses on their networks that have been reported in the previous 24-hour period. ISPs then inform their customer that their computer appears to be compromised and provide advice on how to fix it. Measures to ensure that customers follow this guidance would seem to be a useful initiative for the immediate-term.
There will be substantially more service delivery via the Internet as efficiency gains are sought. This will change the relationship that citizens have with government. Greater use of cyberspace will mean that security will have to be addressed as part of the social contract. There must be assurances around protection of private information and of digital identities and as government agencies deliver more services online, there must be an obligation on those agencies to educate their customers on how to access information securely and how to behave online.

The time has probably come when some form of increased regulation is required; for example, mandating the incorporation of security measures such as firewalls and anti-virus software as conditions of purchase and conditions of sale of computer systems, and ensuring that customers remedy infected systems. Whilst such measures could be viewed by some as an infringement of civil liberties, they would improve both individual and collective security at a low cost, given the failure by many members of the public to date to take even rudimentary security measures to protect themselves on the Internet. Their failure to do so in turn increases the threat to others in cyberspace as individuals’ computer systems become compromised and often utilised in cyber intrusions against others. Furthermore, regulation around mandatory data breach disclosure could be pursued to appropriately protect information held and provide a level of assurance that the information is being protected; as well as mandating proactive testing of networks, applications and systems, especially those deemed to be systems of national interest.

**Government Interaction with Industry**

Industry is not only a vital enabler of Australia’s economic prosperity, global presence and influencing capability on the world stage, it also employs the bulk of Australia’s cyber related intellectual capital and cyber technical expertise. Industry is also a vital part of the all-important cyber education and awareness campaign with the general public. More
importantly, the dynamic nature of the cyber threat is such that it will demand a highly innovative response to deal with it. Innovative and dynamic responses have not been the hallmark of governments in the past; rather, it is industry that has demonstrated innovation and flexibility in the face of commercial challenges and opportunities. Government must harness these qualities in dealing with the cyber threat. Industry is, therefore, a key partner in building national capabilities to deal with cyber threats.

In the short-term, industry should be the most important focal point for government. The Government needs to determine just what constitutes the nation’s cyber-industrial complex and ensure its security. Australia must also address the supply chain threat, where equipment procured may be compromised before it has even begun to be operated. However, engaging with industry can be a complex task, especially as industry’s roles within the cyber domain are varied. In some roles industry finds itself on the front line for cyber threats - the first defender and the first responder - and the Government, therefore, has a vested interest in ensuring that industry is well-placed to assist it with securing the cyber domain. Furthermore, the key government operational agencies – DSD, ASIO, AFP and AGD – will not have the capacity to support all government agencies and industry when suffering a substantial cyber event. They will need the additional capacity of industry.

With respect to cyber security, government and industry are in a co-dependent relationship. Robust and agile cyber security depends on a deep understanding of technological innovation and robust information sharing. Understanding the complexities of this and having a mature dialogue about roles and interdependencies will take time. Improved dialogue and involvement of all relevant parties will lead to better articulation of government and industry roles in cyberspace with sufficient granularity to operationalise their efforts. Improved dialogue and direct engagement should also occur between government and senior business leaders and board members.
A good start has been made and government’s responsibilities are becoming clearer as the capabilities of the CSOC and CERT Australia emerge; these new institutions are in nascent form but already functioning well. The CERT Australia will inevitably grow and the question of whether it remains within the AGD or becomes a separate agency will need to be addressed. Whilst some companies and sectors have formed their own CERTs, larger companies and sectors of industry should be encouraged to do likewise in order to build a network of CERTs within Australia.

Questions have also arisen regarding the need for collocation and integration of the CSOC and CERT as well as the cyber security capabilities of ASIO and the AFP to ensure greater cooperation, and more importantly, better integration of ideas and thinking. Whilst Defence agencies are highly capable, there have been instances where Defence thinking has been shown to benefit from alternate, non-defence, approaches. Recent exercises have highlighted some limitations arising from the separation of the CSOC and the CERT.

Government needs to communicate its incident response and crisis management arrangements from all sources so that industry is aware of the decision-making process and can situate itself in this process to be an effective partner in countering cyber incidents. For example, the roles of CERT Australia, the Trusted Information Sharing Network (TISN), the CSOC, and the AFP and ASIO cyber capabilities, and the value that these different organisations can bring to players impacted by a cyber event are not well articulated and, hence, not well understood. While this is work already underway by the AGD through the CERT and DSD through the CSOC, more can be done by widening the base of industry that is included in the regular exercise and training programs of Government agencies to improve their understanding.

Furthermore, industry requires greater access to low-end sensitive information to better respond to cyber security events. Currently, industry does not have access to threat
information gleaned by the CSOC and provided to ASIO, AFP and CERT Australia. However, industry would have to demonstrate that it could appropriately manage such access before being provided with such.

Government expects that industry will provide a safe, secure and resilient cyber infrastructure for all Australians, which includes:

- implementing appropriate procedures to develop and maintain network system resilience;
- developing capabilities and procedures to respond to attacks on network integrity;
- implementing appropriate procedures to protect personal and sensitive commercial information; and
- educating users on the need for enhanced security measures to deal with cyber issues.

In turn, industry expects that government will address the following issues of concern:

- Requirements determination, a perennial problem, with respect to ‘short life-cycle capability.’ Industry needs to be more involved in the requirements determination process.
- Government needs to determine which environments demand a rapid response, such as remediation to critical infrastructure, and institutionalise partnerships with industry and specific companies to address potential solutions.
- Governments need to allow global companies to collaborate internationally within themselves, and indeed, where relevant, across companies.12

12 For those global companies that operate in multiple countries, information sharing is crucial and more could be done at government-to-government levels to improve that, especially in relation to removing inhibitors produced by anti-trust laws and International Traffic in Arms Regulations (ITAR) restrictions in the US, for example. Multinational companies can provide a global view, using their complementary systems to better address threats. Government incentives and mechanisms can help collaboration across
Australia’s Response to the Cyber Challenge

- Government needs to identify research and development priorities that will provide industry with a better understanding of the government’s focus.

- Government committees can tend to view industry as a source of information as part of an internal and upwards reporting process and provide little information of value back to industry.

Australian companies that are members of the Defence Industry Security Program are required to comply with several security manuals. However, these companies are not provided access to the DSD-managed online site (‘OnSecure’) that provides information security advice to government agencies only. It is difficult to see how these companies can be expected to protect sensitive information to Defence standards if they don’t have access to DSD’s information security advice; even more so if they are to play a critical role in responding to cyber threats in future.

A significant challenge for government is that the private sector is not homogenous; it addresses issues of capability and liability in significantly different ways. Any development of a cyber security framework must take into account this lack of homogeneity and the different private sector conceptions of appropriate action. Cyber capabilities across both government and the private sector are not the same: it is important to identify where the better practices and better skills reside, and use these as the basis for championing the change. Industry has a lot of capability that can be used to support government intent. As with cross-government coordination, there is a need for a clearly enunciated mid- to long-term strategy and associated guidance and plans to provide greater coherence in the Government’s partnership with industry in a whole-of-nation approach to cyber security. This issue is discussed further, later in this report.

---

national boundaries; but if they don’t exist, there will be less likelihood of inter-company collaboration. One possible approach might be for Government to provide an overarching trade agreement to allow Australian industry to talk to its US counterparts.
As previously noted, the Government intends to reach out through the ISPs and other third parties that have face-to-face dealings with consumers. The voluntary ISP code of practice released in June 2010 (and implemented in December 2010) will assist in improving the security of individuals, where it is enforced. The need for legislation to back up the voluntary code of practice should be examined as a matter of priority; government needs to provide some legal cover or indemnity to industry where it acts on behalf of government requirements. Furthermore, many companies will not adopt standards or practices if they cannot see any cost or competitive advantage in doing so. Regulatory frameworks and compliance processes will institutionalise the needed change. Improved security will then flow through to both industry and the wider public. However, regulation needs to be developed with a deft and light touch.

This tends to suggest the need for some form of public-private partnership. To be effective, any such partnership would need to provide three capabilities essential to cyber security – detection (define, identify and watch for behaviours of concern); protection (ensure compliance with the partnership’s security standards, sanctioning those who fail to comply); and response (provide a means to conduct forensic examinations following disruptions, analyse vulnerabilities, fix security shortcomings and effectively attribute attacks to their perpetrators). An option to improve Government and Industry partnering in the cyber environment is discussed later in this report.

**Government Interaction with International Partners**

The Government has a responsibility to shape the international discussion on cyber and to engage with like-minded nations on a host of issues, such as technical standards and acceptable legal norms regarding territorial jurisdiction, sovereign responsibility, and use of force. Cyber is an issue that must be tackled globally; it should be effected through international norms and behaviour, not through more
treaties. However, it does appear easier to develop an international accord on cyber crime than on nation-state behaviour and warfare. Greater determination on achieving international agreement in dealing with cyber crime is warranted in the first instance.

International norms could, for example, treat Distributed Denial Of Service (DDOS) attacks like chemical weapon attacks because of the low cost of entry and inability to discriminate – that is, they are never admissible under international law. Under such a norm, irrespective of whether a DDOS attack was state-sponsored, state-permitted, or carried out by the state apparatus, it would be viewed as a state attack. A second norm might be that national power grids and other critical infrastructure can be attacked only in an openly-declared state of ‘kinetic conflict.’ A third might be that financial grids are to be treated in similar vein to hospitals – never to be attacked and never to be subjected to espionage because no transient combat advantage can accrue in proportion to the damage caused. In essence, international agreements to set power grids, the financial sector, and other components of civilian infrastructure off limits would be in the interests of most nations. Through norms and international agreements such as these much of the current malevolent activity, which reportedly is state-sponsored, might be contained allowing other cyber security issues to be more visible and thus easier to deal with.

Australia has established solid engagement and beneficial relationships within some forums with respect to cyber security; e.g., with the Asia-Pacific Economic Cooperation (APEC). However, a wide range of cyber issues is now being discussed across a number of other international forums. The challenge will be to maximise opportunities for cooperation across all of these bodies. Agreeing on acceptable international norms will not happen quickly, but this is not a reason not to engage wholeheartedly. In interacting with international partners, it is absolutely critical that Australia presents a coordinated and well-understood ‘single view’ of its
national cyber aspirations. The Australian Government announced its intention to accede to the Council of Europe’s Convention on Cybercrime on 30 April 2010. Australia is currently in a good position to comply with the majority of obligations under the Convention. From a regional perspective, Australia might support any cyber security initiatives proposed by the ASEAN Regional Forum (ARF) or the Council for Security Cooperation in the Asia Pacific (CSCAP).

While adversaries may act alone, Australia has great advantage in its established trust relationships with allies. The nation can, therefore, develop sound international strategies in seeking to counter the threat from the most serious state-based adversaries. Government-to-government, multilateral behaviour must be the way of the future. National CERT to national CERT interactions can underpin these relationships. These CERT-to-CERT relationships will mature and be important elements of any framework, but they will depend on a willingness to share information, not just to receive it. The task ahead is to develop knowledge and capability that can be shared in these forums.

The decision with respect to sharing information rests with the agency that has sourced the information. There is a need to improve such information sharing, perhaps assisted by a risk methodology for determining criteria around information sharing with industry. Some form of a national interest test will need to be developed in the near future to better accommodate this.

A priority for the international technical agenda around the Internet, in shifting focus to security, could be to address the most troubling vulnerabilities:

- the Internet Protocol, which guides data from source to destination across the Internet;
- the Domain Name System, which translates IP numbers into recognisable Web addresses;
Australia’s Response to the Cyber Challenge

- the Border Gateway Protocol, which provides the connection between networks; and
- evolutionary and revolutionary consumer-driven technologies, which when implemented, change the security posture of current systems.

The three protocols do not have built-in mechanisms to verify the origin or authenticity of information sent to them, leaving them vulnerable to being spoofed or otherwise manipulated by malicious actors.

An option worthy of consideration is to develop a mechanism for an annual status report on the key issues around international cooperation, what is being done about them, how the actions are being tracked, and what is new. Such an approach could be a part of the proposed mid- to long-term strategy and associated guidance and plans discussed later in this report.

It was pleasing to note the agreement announced at the November 2010 AUSMIN talks which stated that Australia and the United States intend to promote a secure, resilient and trusted cyberspace that assures safe and secure access for all nations and that both countries are committed to work together to advance the development of shared international norms for cyberspace.13

Cyber-Related Law Enforcement

The main challenges for cyber-related law enforcement revolve around the rapid advancements in technology (and the ability of criminal networks to exploit them), the lack of utility of some traditional legal frameworks, the lack of community understanding on what cyber crimes are and the limited resources provided to address law enforcement. In one sense, the legal framework challenge posed by the cyber environment parallels that of terrorism threats a decade ago,

---

where similar issues prevailed around crime prevention, law enforcement, the judiciary and juries. The challenges of the criminal justice system in dealing with terrorists were articulated and dealt with. A similar approach will be required in relation to cyber threats.

Cyberspace is increasingly impacting legal frameworks related to copyright, electronic transfer activity, international law, and Law of Armed Conflict (LOAC). However, national legislation may mean little if it is not part of an international legal framework. Complicating this issue is the changing nature of operations in the cyber environment. For example, legislation does not exist to enable companies to carry out ‘active defence’ against a cyber intrusion, although it would seem that many companies are in fact conducting such activities as passive defence measures are proving to be inadequate. Legal clarity is needed although it will be difficult to achieve in this area where issues of national interest and commercial interest do not necessarily align.

A significant issue is the lack of a sophisticated debate over just what constitutes cyber crime and therefore what are the appropriate jurisdictional frameworks. This, in turn, results in a challenging environment for law enforcement agencies, many of which lack adequate resources to tackle the issue. For example, the AFP’s High Tech Crime Operations capability comprises only a small specialist investigative capacity to support the identification, investigation and prosecution of complex technology crimes. Observations from the strong cyber investigative capability of the US Secret Service indicate that even a small amount of additional resources could achieve disproportionately greater results for the AFP, including the normalisation of cyber behaviour and skill sets across all federal police agents through improved education and training.

Law enforcement agencies and industry need to cooperate to improve the sharing of information. Industry can provide law enforcement agencies with information on new and emerging threats, including the modes of attack. Partnerships and
strategic alliances are critical to crime prevention – no single agency or organisation can operate effectively in isolation. Any national framework for the future will need to be championed by the Prime Minister and implemented via the Council of Australian Governments (COAG).

Significant frustration has been expressed by industry at the low prosecution and conviction rates. Presenting evidence in court can be a challenge, depending on the computer literacy of judges and juries. Investigators and technicians must have a sound understanding of the technical concepts and be able to explain those to a judge and jury in a way they can grasp. Systemic weaknesses include not only the computer literacy of judges and juries, but also those of impacted agencies and organisations in their understanding of what information to collect and how to preserve evidence that can be subsequently used in the judicial process. A significant education and awareness program is needed in this area.

INDUSTRY’S ROLES AND RESPONSIBILITIES

A number of areas of industry have a sophisticated approach to cyber security and a mature information-sharing relationship with government. Those relationships are with ASIO, AFP, CERT Australia and the CSOC. These relationships provide a solid foundation on which growing roles and responsibilities of industry can be developed. However, when under stress, people default to their tried and true relationships and not necessarily those driven by a specific threat vector. For example, the current interim cyber security plan is considered by many to be too different from tried and tested ‘all hazard’ risk management structures to add any value. Indeed, some agencies have ignored it as they do not understand how it works nor how it adds any value.

Significant weaknesses within industry need to be addressed, including the lack of effective governance, poor understanding of the cyber threat, and the sharing of data. Many boards fail to understand and, therefore, address the
business risks in the cyber environment. Many small businesses adopt the ‘it won’t happen to me’ attitude, placing themselves and others at risk as their systems are compromised and exploited through cyber intrusions. Increasingly, operational risk and information technology security must be seen as intrinsically linked. Benchmarking, risk mitigation, regulatory and legal compliance are the issues that need to be articulated in any governance framework. In addition, work is needed to clarify tort liability to protect those companies that cooperate with government in matters of national interest.

In many instances governance has been improved by aggregating physical, information, transport, environmental and cyber security under a Chief Security Officer. Whilst this is becoming an established function in many overseas businesses it has yet to gain significant foothold in Australia.

Technological advances will result in new vulnerabilities; as a consequence, baseline security provisions may need to be mandated and policed by Government. Such provisions would need to address security, capability and awareness (especially at board level), data management, industry skills and privacy considerations.

Many business organisations are slow in detecting and responding to incidents, with most data breaches being discovered by external parties, often only after a considerable period of time has elapsed. Default, stolen and weak credentials and insider threats appear to be the main problem. While this is neither new nor expressly cyber-related, the amount of compromise or damage that can ensue, given the vast amount of information now stored that an insider can access, is growing exponentially. Businesses share elements of threat vectors; however, the magnitude of the effect or impact is often not shared. A mechanism to improve information sharing across industry should be explored for without improved shared situational awareness, cyber defences will be compromised.
PEOPLE, CULTURE AND WORKFORCE ISSUES

There are significant people and workforce challenges associated with cyberspace. Australia, like other western societies is experiencing a decline in science, engineering, and mathematics skills. There are concerns that current structures and processes will not be able to address the people and workforce demands effectively for the future. The nation’s education system must, therefore, place new emphasis and priority on attracting and educating creative and innovative young men and women with the necessary skills to deal with this technologically-based society and resulting cyber threat.

The Center for Strategic and International Studies (CSIS) report, A Human Capital Crisis in Cybersecurity notes that ‘The cyber threat to the United States affects all aspects of society, business and government, but there is neither a broad cadre of cyber experts nor an established cyber career field to build upon, particularly within the Federal government’. A similar situation exists in Australia with a large percentage of students in this field being foreign students, merely studying in this country. As a result, government and industry will face significant challenges in recruiting and retaining a cyber workforce as the demand for such skills grows.

Cyberspace-oriented education must reach down to the primary-school level and continue on through higher education. The capability of key universities that can provide important advanced cyber skills must be harnessed in order to ensure there is sufficient capacity and resourcing for preparing the future cyber workforce.

Cyber security awareness, training and education require a coordinated national effort and need the corresponding resources to be allocated. There is a need, not only for high-level information security training and certification, but also for a higher degree of cyber acumen and awareness coupled with new cultural sensitivity to meet new requirements and expectations related to collaboration and transparency. All
organisations will need not only to educate their workforce, but also to underscore the expectation that all employees are accountable and responsible for safeguarding and sharing information under their purview, regardless of their position or level in the organisation. These actions imply a cultural shift of some significance.

Education and awareness across the public, business and government must also be aligned; the systemic risks and cascading effects across myriad interdependencies means this alignment is no longer optional. In this respect, it might be prudent to examine the notion of a virtual cyber academy, as discussed later in this report.

**THE NEED FOR A NATIONAL CYBER STRATEGY AND FRAMEWORK**

Whilst progress in implementing the Government’s 2009 Cyber Security Strategy has been noteworthy, Australia is not keeping pace with the growing threat and as a result is placing the collective and individual security of the nation’s people at risk. Whilst a number of people have expressed the view that a catastrophic event, a ‘Cyber 9/11,’ would be required to prompt any significant broadening or acceleration of the Cyber Security Strategy, the authors are of the view that acceptance of such a view would be defeatist.

The concept of working together in a cohesive and coordinated fashion is not new for the Government community. Counter-terrorism is one obvious example of a significant, effective, whole-of-government effort. The Cyber Security Strategy is simply another issue-driven means of focusing national efforts despite the complexity and scale of the cyber challenge. The nature of this threat, however, is that Government must first focus on cyber as a unique concept so that it can build the governance mechanisms to ensure that resources are focused and appropriately invested to meet the threat in the short-, medium- and long-terms.
Australia’s Response to the Cyber Challenge

Improvements in Australia’s national response to the cyber threat necessitate changes in the current strategy and plan, as well as in the structure and process used to implement the plan and to operate in cyberspace. The nature of these changes is discussed below.

Cyber Strategy and Plans

The current Cyber Security Strategy has a horizon of only a few years. It has been difficult to ascertain what actions are taking place across government and industry in relation to Cyber security and what the longer-term goals are. In other words, many pieces are visible, many are not and the overall integrated ‘picture’ is missing. This statement is not meant to denigrate any part of government; indeed the actions taken to date are excellent. Rather, it is meant to indicate that the actions taken to date have helped highlight the scale of the problem and that more is needed to be done in order to address the challenge ahead.

Individually, departments, agencies and interest groups are experiencing difficulty in indentifying the full breadth of the challenge and communicating that challenge to government, industry and the public. What is lacking is an integrated whole-of-nation, government-led long-term National Cyber Strategy and Plan (as a subset of the National Security Strategy) with defined responsibilities, identified priorities and dedicated resources that recognises the scale of the cyber challenge and the need to address that challenge in a more comprehensive manner. Without such an approach national efforts will not be fully coordinated and, as a result, will not be as effective as possible.

Australia needs to gain a shared understanding of what it wishes to achieve in the cyber environment over the next decade and to develop a collective concept and a resourced plan of how it intends to achieve that. Such a plan would support improved partnering between the Government and Industry and would assist in improving the public’s
understanding of what will be done to improve the nation’s security in cyberspace.

Whilst Australia naturally looks to the United States and the United Kingdom to compare methods for addressing the cyber threat, there are lessons closer to home - from the Department of Defence’s strategy and planning implementation framework - that could be applied to complex systems-level challenges in the wider national security space, in particular for cyber security. The Australian Department of Defence’s approach broadly comprises a strategy, a concept of operations and a resultant capability plan with dedicated resources. Whilst Defence plans are subject to ongoing change, the planning process affords a shared understanding and provides a focus for investment that aims to maximise the return on the investment of government and industry funds.

*A Proposed Strategic Cyber Framework*

The following cyber framework could be used to focus and coordinate actions within Australia to address the growing cyber threat. The proposed framework has three main elements; strategic guidance, an implementation plan and a roadmap to guide and monitor implementation, as illustrated in Figure 2.
Figure 2: Proposed Strategic Cyber Framework

The Strategic Guidance element would comprise a longer-term enhanced National Cyber Strategy, a Cyber Concept of Operations and a Cyber Capability Plan.

The National Cyber Strategy would provide a 10-year vision of what needs to be achieved in the security and management of cyberspace in Australia. It could expand on the excellent Cyber Security Strategy developed by the AGD, providing further clarity on the roles and responsibilities across Government, in particular that of the NSA and DSD’s CSOC, and provide a vision of how Australia will function effectively in a future challenging cyber environment, enabled by recent initiatives such as the National Broadband Network. It could broaden the existing cyber strategy focus on the availability, integrity and confidentiality of Australia’s ICT to one which focuses on the wider cyber environment and emerging challenges. Most importantly, it could highlight the need for a flexible and innovative approach to dealing with threats that are as yet undefined and provide the vision of how those characteristics can be enhanced in the Australian environment. The development and implementation of a National Cyber Strategy provides an excellent opportunity to
strive for such an environment; however, the implementation of such a strategy could also pose a significant risk if it was too bureaucratic and in turn stifled existing innovation activities being led by individual departments and agencies.

The key strategic themes that emerged in this study suggest a focus for a National Cyber Strategy on five fundamental objectives:

- First, it must comprehensively understand the threat, and continually reduce cyber vulnerabilities.
- Second, it should build a credible counter-attack capability, notwithstanding the very difficult challenge of attribution.
- Third, it must actively pursue continuous technology discovery, with increased emphasis on research and the necessary funding provided.
- Fourth, it must address much-needed culture and behaviour changes.
- Fifth, it must consider how Australia should relate, align and integrate its cyber strategy and capabilities with those of its allies and friends.

**A Cyber Concept of Operations** would describe the characteristics of the proposed cyber system from the viewpoint of a user of the system. It could:

- Establish a shared understanding of the range of future cyber environments in the national security context.
- Provide the thread of logic - the shared understanding of how Australia will 'operate'; i.e., deal with the emergent threats and capitalise on opportunities in the future cyber environment.
- Guide the development of a government, industry, public and individual team culture to deal with the challenge.
• Guide research, experimentation and innovation priorities to support improved national cyber capabilities.
• Inform workforce planning.
• Inform the cyber security plan as a component of the National Security Capability Plan. 

A Cyber Capability Plan would provide a forward-looking view of the capabilities that will be developed or acquired to improve the national ability to operate effectively in the cyber environment. Such a plan would be a subset of the foreshadowed National Security Capability Plan. It is hard to imagine how defence industry would function and invest in the absence of a Defence Capability Plan. Yet this is the situation faced by industry in dealing with the emerging cyber market. A capability plan would provide improved certainty of resources and enable industry to target its capability investment in support of Government goals, thus providing the environment that would promote effective partnering between Government and industry in dealing with the cyber threat and associated challenges.

The second element of the Strategic Cyber Framework, the Implementation Plan, would focus on the national ability to operate, innovate and educate in the cyber environment. The Plan would articulate the current and future roles of the CSOC and CERT Australia and how they would operate and cooperate with Government Agencies and Industry. It would outline a coordinated innovation and experimentation program that would link such activities across Government with the wider industry base. Finally, a coordinated education and training program would guide the development of the future cyber workforce and assist in engaging the behavioural

---

54 The Labor Party 2010 Election campaign stated that ‘a re-elected Gillard Labor Government will develop the first National Security Capability Plan to ensure all non-defence national security agencies agree on the security risks facing our country, and the capabilities required to respond to those risks in the future.’
and thus cultural change essential to improving Australia’s ability to function in the emerging cyber environment.

The third element of the Strategic Cyber Framework, the Roadmap, would address specific actions (including leadership and implementation responsibilities and timelines), together with the prioritisation of actions and the allocation of resources. With any roadmap, progress needs to be measured; and a system of key performance indicators (KPIs) should be included in the roadmap to measure progress and to trigger 'mid-course corrections' as necessary.

**Structure and Process Change Options**

Governments in general are not well structured to deal with the nature of emerging cyber issues which will require highly innovative, integrated and dynamic responses and defensive actions. In the case of Australia, there is a need to increase the focus on cyber issues across government and industry. Australia has a federated response to cyber threats via the CSOC, where agencies can assert their authority over a particular issue and take the lead, with other agencies in support. However, a genuinely unified national response framework is still lacking.

The 2008 decision to establish the NSA Office within PM&C was a significant step forward in integrating national security actions. As noted previously, the NSA Office would be best placed to play a greater role in integrating cyber functions across the broader national security functions. With this in mind consideration could be given to:

- appointing a Minister with oversight responsibility for cyber issues, together with a ministerial committee such as a sub-group of the National Security Committee of Cabinet;
- establishing a limited-term Deputy Secretary position within the NSA’s office to be responsible for increasing the focus on cyber matters and broaden the role of, or provide an additional, CIO position to address private
sector issues in addition to the existing cyber policy coordination role of the current CIO;

• establishing cyber planning and coordinating committees in addition to the CSPC Committee to address Government aspects, and corporations and their interface with Government; and

• establishing a cyber sub-committee under the Joint Standing Committee on Foreign Affairs, Defence and Trade.

Whilst the structure and process changes above could assist in the development and execution of an integrated cross-Government National Cyber Strategy, they will not necessarily address the need for greater Government and Industry cooperation and coordination. Cyber defence will be an ‘around-the-clock’ mission requiring absolute cooperation among all parts of government, businesses, the public and allied nations.

Like most western societies, Australia will be faced with a situation where the best defence is all-encompassing, where most of the talent is in the private sector and where the majority of the technological advance occurs in the private sector. To support such cooperation, a future ‘GOCO’ - a Government Owned, Contractor Operated Company - is proposed.\textsuperscript{15} The GOCO could become the Cyber Defence agent of the Government; it would comprise government agencies and a range of industry members. Whilst cyber attack would remain a solely government function, protected by the usual national security standards and procedures, the Government could ‘out-source’ a significant proportion of all its

\textsuperscript{15} GOCOs began in World War II to address the sudden need to expand the armed forces. To facilitate the necessary expansion, the government ultimately provided most of the needed capital. In some cases, the government built plants, stocked them with the necessary equipment, and hired a contractor to operate the plant. Such facilities became known as government-owned, contractor-operated (GOCO) plants. Since the war, GOCOs have been used for a number of functions ranging from advanced research and development to the manufacturing of war materials.
wider (non–military) national cyber defence efforts to the company. The advantage of a GOCO would be that it could:

- engender close government and industry teaming;
- ensure government control of important activities;
- provide capital where otherwise there would be none;
- allow commercial-style procurement and hiring practices; and
- obviate the oftentimes slow and painful process of government structural change.

The underlying principle of the GOCO has some similarities with the Defence Rapid Prototyping, Development and Evaluation (RPDE) Program, a collaborative venture between the Australian Department of Defence and industry.\(^{16}\) The Defence Department’s RPDE program should be examined for lessons that could be applied to government and industry teaming in the cyber environment.

In addition to the reactive measures in place and proposed, greater proactive action will be required. Measures should include actions to transform behaviour and thus culture, promote greater teaming and collaboration with wider acceptance of accountability for improved cyber security, and accelerated innovation and development of cyber responses. Proactive action could be supported through some form of innovation centre, possibly a National Security Innovation Centre, with an initial focus on cyberspace. Such an innovation centre, coupled with improved cyber education and training, could support accelerated systemic changes needed to address the growing threat.

An option that could be considered by Government as a part of the proposed innovation centre would be to include a ‘Cyber RPDE Program’ as a demonstrator of the GOCO

---

\(^{16}\) Faced with a need for rapid innovation and greater collaboration in the Network Centric Warfare field, Defence established the RPDE Program in 2005. The Program has proven highly beneficial in improving teaming between Defence and Industry.
model. The demonstrator could be used to drive research and innovation in the cyber environment, establish improved government and industry teaming, and assist in the education of government and industry in cyber issues.

Improved cyber education and training could be provided through a virtual cyber academy, a cyber range and a cyber Cooperative Research Centre (CRC). The creation of a cyber academy could be achieved virtually by linking universities and relevant educational institutions to develop the underpinning cyber skills base in Australia.

This study has identified a number of actions that should be considered to address the cyber challenge. These actions are summarised in Annex B. A key consideration regarding any recommended actions is that of timing - the gap between threat and response capabilities is growing. In the aftermath of the global economic crisis all governments are faced with increasing financial pressures. Projected growth in social security and health costs will only exacerbate these financial pressures in the future. If Australia does not increase its focus on cyberspace, the threat will grow faster than any response and the cost of addressing the larger threat gap in the future will increase, possibly exponentially. Any delay in taking action may prove unaffordable in the long-term.

Acting early demands a number of specific evolutionary actions that should be taken in the near-term, such as continuing to build on the current cyber programs but with some process and structural change, greater clarity over roles and responsibilities, and additional resources, as discussed earlier. A number of transformational activities that should be carried out over the medium- and longer-terms are also needed, involving proactive measures such as a National Security Innovation Centre, a virtual Cyber Academy, a Cyber Test Range, and a cyber Cooperative Research Centre. However, the timing imperative to address the growing gap between threat and response capabilities means that the seeds of these transformational actions must be sown in the near-term.
Figure 3 illustrates the proposed actions in the context of the timing imperative: the reactive and proactive measures, the role of an innovation centre, and improved education and training, all of which need to be progressing in 2012 in order to accelerate systemic change and address the growing threat gap with a mature future cyber system in 2020.

![Diagram of proposed actions and timeline]

**Figure 3: Proposed Actions**

A significant challenge with the implementation of the proposed Cyber framework is the measures of success. Suggested measures of effectiveness discussed during the workshops are contained in Annex C.
CONCLUSIONS

The Kokoda Foundation Cyber Study sought to answer two fundamental questions: are we doing enough to address the growing threat to our national and individual security in the cyber environment; and if not, what do we need to do?

The study concluded that:

• We are not doing enough:
  o Whilst progress in implementing the Government’s 2009 Cyber Security Strategy has been laudable, we are not keeping pace with the growing threat and as a result we are placing our collective and individual security at risk.

• We need to:
  o Develop a whole-of-nation, government-led integrated long-term National Cyber Strategy and Plan (as a subset of the National Security Strategy) with defined responsibilities, identified priorities and dedicated resources.
  o Assign the lead to coordinate cyber-related security issues across government to the NSA.
  o Continue to build on the current cyber programs but with some process and structural change to ensure the cyber threat is understood and cyber vulnerabilities are reduced, a credible counter-attack capability is developed, continuous technology discovery is pursued, culture change is effected, and alignment with key allies is achieved.
  o Accelerate systemic change through a suite of proactive measures such as the proposed National Security Innovation Centre, a virtual cyber academy, a cyber test range, and a cyber CRC. This will help to normalise cyber as a part of everyday activity.
This study concluded that the cyber challenge confronting Australia is complex and, while unique in many aspects, it should be addressed in similar manner to other national security challenges, through existing national security structures but with increased focus and resourcing, guided by a more coherent strategy and plan. The central cyber policy and coordination body (whether this is the NSA or the new Cyber Policy Coordinator) will need to be disencumbered from the attendant bureaucracy around the current crisis management arrangements as cyber responses must operate at network speed, which underscores the pivotal operational role of the CSOC.
Annex A

DEFENCE SIGNALS DIRECTORATE’S TOP THIRTY-FIVE MITIGATION STRATEGIES

Over 70% of the targeted cyber intrusions the Defence Signals Directorate (DSD) responded to in 2009 could have been prevented by following the first four mitigation strategies listed in the Top 35 Mitigation Strategies:

• Patch operating systems and applications using auto-update.
• Patch third-party applications such as PDF readers, ActiveX objects and web browser plug-ins.
• Restrict administrative privileges to users who need them.
• White-list approved applications.

The Top 35 Mitigation Strategies are ranked in order of overall effectiveness. Rankings are based on DSD’s analysis of reported security incidents and vulnerabilities detected by DSD in testing the security of Australian Government networks.

1. *Patch the operating system* and applications that have a corporately manageable auto-update feature.
2. *Patch third party applications* such as PDF readers, ActiveX objects and web browser plug-ins.
3. *Minimise administrative privileges* to only users who need them.
4. *Application white-listing* to help prevent unapproved programs from running.

---

5. **Host-based Intrusion Detection and Prevention System** to identify anomalous behaviour such as process injection, keystroke logging, driver loading and call hooking.

6. **Workstation conversion and sanitisation of Microsoft Office files**; e.g., Microsoft Office Isolated Conversion Environment (MOICE).

7. **White-listed email content filtering** preferably converting and sanitising PDF and Microsoft Office files.

8. **Gateway** with a split DNS server, an email server, a password authenticated web proxy server and a firewall preventing workstations directly accessing the Internet.

9. **Data Execution Prevention** using hardware and software mechanisms for all compatible software applications.

10. **Antivirus software** with up to date signatures and heuristic detection capabilities. Use gateway and desktop antivirus software from different vendors.

11. **Sender Policy Framework** to help block incoming spoofed emails, and to help prevent spoofing of your domain.

12. **Audit reconnaissance tool usage**; e.g., the system executables ipconfig, net, net1, reg, gpresult and systeminfo.

13. **Restrict access to NetBIOS services** running on workstations and on servers where possible.

14. **Application based workstation firewall** to protect against malicious or otherwise unauthorised incoming network traffic.

15. **Network segmentation and segregation** into security zones to protect high value assets using routers, switches and firewalls.

16. **Centralised logging** using a synchronised time source, combined with regular log analysis.

17. **Disable unrequired operating system functionality**; e.g., disable or restrict services such as Remote Desktop, harden configuration of file and registry permissions.
18. **Application security configuration hardening** especially for Microsoft Office applications, PDF viewers and web browsers.

19. **Application based workstation firewall** that white-lists applications allowed to generate outgoing network traffic.

20. **Web domain white-listing** (more proactive and thorough than black-listing) for domains that use HTTPS/SSL encryption.

21. **Web content filtering** using a combination of signatures, heuristics, and white-listing allowed content types.

22. **Two factor authentication** for access to sensitive information repositories.

23. **Removable media control** including storage, handling, white-listing allowed USB devices, encryption and destruction.

24. **Web domain white-listing** (more proactive and thorough than black-listing) for all domains.

25. **Disable LanMan** password support on workstations and servers.

26. **Block attempts to access web sites by their IP address** instead of by their domain name.

27. **TLS encryption between email servers** to help prevent legitimate emails being captured over the wire and used for social engineering.

28. **Randomised local administrator passwords** that are unique and complex for all computers.

29. **Gateway blacklisting** to block access to known malicious domains and IP addresses.

30. **Network-based Intrusion Detection System** using signatures and heuristics to identify internal network traffic such as enumeration of shares and users.

31. **User education** about web threats, focusing on identifying spear phishing socially engineered emails.
32. *Network-based Intrusion Prevention System* using signatures and heuristics to identify *internal* network traffic such as enumeration of shares and users.

33. *Rolling network capture* to perform post-incident analysis of inevitable successful intrusions, to determine the adversary’s techniques and assess the extent of damage.

34. *Network-based Intrusion Detection System* using signatures and heuristics to monitor *external* network traffic (focusing on outgoing traffic).

35. *Network-based Intrusion Prevention System* using signatures and heuristics to monitor *external* network traffic (focusing on outgoing traffic).
Annex B

RECOMMENDED ACTIONS

Develop a whole-of-nation, Government-led integrated long-term National Cyber Strategy and Plan (as a subset of the National Security Strategy) with defined responsibilities, identified priorities and dedicated resources. Assign the lead to coordinate cyber-related security issues across Government to the Office of the National Security Adviser.

- **Strategic Cyber Framework**. There is a need for a mid- to long-term strategy and associated guidance and plans to provide greater coherence in the Government’s approach to cyber security. The proposed National Cyber Strategy and Plan would have three main elements; strategic guidance, an implementation plan, and a roadmap to guide and monitor implementation. The Strategic Guidance element would comprise a longer-term enhanced National Cyber Strategy, a Cyber Concept of Operations and a Cyber Capability Plan.
  
  o The National Cyber Strategy would provide a 10-year vision of what needs to be achieved in the security and management of cyberspace in Australia.
  
  o A Cyber Concept of Operations would describe the characteristics of the proposed cyber system from the viewpoint of a user of the system.
  
  o A Cyber Capability Plan would provide a forward-looking view to the capabilities that will be developed and acquired to improve the national ability to operate effectively in the cyber environment. Such a plan would be a
subset of the foreshadowed National Security Capability Plan.

- Whilst Australia naturally looks to the US and UK to compare methods to address the cyber threat, there are lessons from the Australian Department of Defence strategy and planning implementation framework that could be applied to complex systems-level challenges in the wider national security space, in particular for cyber security.

- **Roles and Responsibilities.** The NSA Office would be best placed to play a greater role in integrating cyber functions across the broader national security functions. With this in mind consideration could be given to:
  
  - appointing a Minister with oversight responsibility for cyber issues, together with a ministerial committee such as a sub-group of the National Security Committee of Cabinet;
  
  - establishing a limited-term Deputy Secretary position within the NSA’s office to be responsible for increasing the focus on cyber matters and broaden the role of, or provide an additional, CIO position to address private sector issues in addition to the existing cyber policy coordination role of the current CIO;
  
  - establishing cyber planning and coordinating committees in addition to the CSPC Committee to address Government aspects, and corporations and their interface with Government; and
  
  - establishing a cyber sub-committee under the Joint Standing Committee on Foreign Affairs, Defence and Trade.
Australia’s Response to the Cyber Challenge

- Resourcing.
  - It is vital to determine just what the baseline investment should be as a part of a national security capability plan in order to give some certainty to those departments responsible for improving cyber security and awareness. For example, whilst the AGD CERT function is funded to establish the CERT, it will clearly need to be increased significantly as the CERT function grows in response to the increasing demand for its services, and as industry provides greater access to the CERT.

  - CSOC funding and capabilities should be leveraged to the fullest extent possible by those agencies with embedded staff in the CSOC – such as CERT Australia, ASIO and the AFP. These agencies will be less susceptible to being flooded with data and requests if they are able to exploit the synergies of being located together with the CSOC.

  - Observations from the strong cyber investigative capability of the US Secret Service indicate that a small amount of additional resources could achieve disproportionately greater results. For example in the case of the AFP, a small increase in resources could enable the normalisation of cyber behaviour and skill sets across all federal police agents through improved education and training.
Continue to build on the current cyber programs but with some process and structural change to ensure the cyber threat is understood and cyber vulnerabilities are reduced, a credible counter-attack capability is developed, continuous technology discovery is pursued, culture change is effected, and alignment with key allies is achieved. Proposed Changes include:

- **Critical infrastructure.** Consideration should be given to mandating progressive changes to critical infrastructure and SCADA systems as they are upgraded or replaced. For example, significant improvements in system protection could be achieved by:
  - disconnecting the power grid and any control system transporting people, managing gas and petrol production or controlling the flow of water from the wider Internet; and
  - mandating credentials for digital identities (if all external interactions needed to be authenticated, it would reduce the potential exfiltration paths as well as potential command and control paths) and mandating cyber security standards for companies commensurate with their size or involvement with critical infrastructure.

- **Communications with Industry and the Public.**
  - Stronger links across AGD, DBCDE, AFP, Treasury and ACCC would seem warranted to enable improved awareness and protection across the entire community, and to ensure that individual messages are consistent with and supportive of one another. The first steps in public awareness have been taken and while Fraud Week, Privacy Week, Cyber Security Awareness Week and others are all effective, greater synergies could be obtained through
closer coordination of the messages behind such events.

- The impending integration of government data systems of agencies such as Centrelink and Medicare and the planned migration to provision of services to primarily online provide the opportunity for government to build a direct online relationship with the vast majority of Australian citizens who will access these online services. Through targeted education programs, the government has the opportunity to shape the behaviours of individuals accessing services online and thus improve security within the broader cyber environment.

- The rollout of the NBN offers a significant opportunity to engage the public to better understand the vulnerabilities that could arise from the significantly increased bandwidth that will be made available and in turn the responsibilities of individuals as well as the ISPs to take appropriate security measures.

- The lack of priority and resourcing has occurred mainly because cyber security is competing rather poorly for the attention of politicians and company boards. Use of institutions such as the Australian Institute of Company Directors and the Risk Management Institution of Australasia should be considered to educate industry executives and politicians. An expanded role for the nascent National Security College should also be investigated.

- Government needs to communicate its incident response and crisis management arrangements from all sources so that industry is aware of the decision-making process and can situate itself in this process to be an effective partner in countering cyber incidents.
Progress is being made by the AGD through the CERT and DSD through the CSOC, but more can be done by widening the base of industry that is included in the regular exercise and training programs of government agencies, and improving industry’s access to certain information, including the DSD-managed online site ‘OnSecure’.

- Businesses share elements of threat vectors; however, the magnitude of the effect or impact is often not shared. A mechanism to improve information sharing across industry should be explored for without improved shared situational awareness, cyber defences will be compromised.

- **Education and Training**
  - Cyber security awareness, training and education require a coordinated national effort and need the corresponding resources to be allocated. All organisations will need not only to educate their workforce, but also to underscore the expectation that all employees are accountable and responsible for safeguarding and sharing information under their purview, regardless of their position or level in the organisation. These actions imply a cultural shift of some significance.

- **Legislation, Regulation and Governance**
  - Greater determination on achieving international agreement in dealing with cyber crime is warranted. Cyber is an issue that must be tackled globally; however, this should be effected through international norms and behaviour, not through more treaties. In interacting with international partners, it is absolutely critical that Australia presents a
coordinated and well-understood ‘single view’ of its national cyber aspirations.

- The voluntary ISP code of practice released in June 2010 will assist in improving the security of individuals, where it is enforced. The need for legislation to back up the voluntary code of practice should be examined as a matter of priority.

- The time has probably come when some form of increased regulation is needed to mandate the incorporation of security measures such as firewalls and anti virus software as conditions of purchase and conditions of sale of computer systems to reduce the number of computers compromised by viruses and malware, and to ensure that ISP customers remedy infected systems. Mandating data breach disclosure and proactive testing of critical systems, networks and applications should also be introduced through regulation.

- Companies are acting in self defence in what is often referred to as ‘active defence.’ The lack of dialogue and clear legal guidance in this arena increases the risk of self defence actions being both illegal and potentially damaging to Australia’s national interests where such activities result in collateral damage to other nations.

- Significant weaknesses within industry include the lack of effective governance, poor understanding of the cyber threat, and the sharing of data. Many Boards fail to understand and therefore address the business risks in the cyber environment. Benchmarking, risk mitigation, and regulatory and legal compliance should all be issues articulated in a governance framework. In addition, work is needed to
clarify tort liability to protect those companies that cooperate with government in matters of national interest.

Accelerate systemic change through a suite of proactive measures such as the proposed National Security Innovation Centre, a virtual cyber academy, a cyber test range, and a cyber CRC.

- The Defence Department’s RPDE program should be examined for lessons that could be applied to Government and Industry teaming in the cyber environment.

- Departments and Agencies outside of Defence do not have dedicated research funds to apply to cyber security. In addition to pure research funding there appears to be a strong case for the establishment of appropriate tools and test capabilities. For example, a SCADA test bed would appear to be a much-needed capability, particularly if developed as a part of a national cyber test range.

- Proactive action could be supported through some form of innovation centre, possibly a National Security Innovation Centre, with an initial focus on cyberspace. Such an innovation centre (possibly based on a GOCO model), coupled with improved cyber education and training, could support accelerated systemic changes needed to address the growing threat. This will also help to normalise cyber as a part of everyday activity.
Annex C

MEASURES OF SUCCESS

Drawing on the report of a workshop that was jointly conducted by the American Bar Association Standing Committee on Law and National Security, and the National Strategy Forum, a number of observations were made regarding measures of success. It will be difficult to say whether a reduction in the number of intrusions detected reflects success in preventing them or a growing capacity on the part of the intruders to evade detection. Nevertheless, there are some realistic measures that the Report suggests could be adopted and that have been modified slightly, such as:18

- Have the number of intrusions into government and industry systems been reduced?
  - What degree of success do government red teams have in penetrating networks?
  - Is the attribution of attackers more effective?
  - Have encryption standards been improved?
  - Does intrusion detection lead seamlessly to immunisation and prevention, such that intrusions by a particular method are a one-time-only occurrence?
  - Has an effective identity management system been adopted?
  - Is the nation more successful in offensive cyber intrusions than its opponents?

---

o Have coordination and agility in responding to events been enhanced in a way that has normalised cyber activities as part of all other activities?

- Has the private sector adopted appropriate security measures?
  o Has the application of patches for vulnerabilities that are known to exist been increased, overcoming previous lethargy that prevented or delayed their application?
  o Are auditing schemes generally in place? Have they resulted in the adoption of generally accepted best practices that embody standards of care that the courts deem significant?
  o Is private sector research and development increasing?
  o Is there an appropriate liability regime in place that allows injured parties to seek compensation for consequential damage?
  o Have ways been found to incentivise resilience?
  o Is more secure system architecture being devised for the cyber domain? What are the prospects for its adoption and implementation?

- Has a doctrine for cyber warfare and response been developed?
  o Do all actors know how to respond to an overt cyber attack that causes physical damage?
  o Do all actors know what the response will be to a covert intrusion?
  o Have the actions that constitute an armed attack been defined and have the procedures around attributing that attack to a nation-state been determined?
Australia’s Response to the Cyber Challenge

- Has the law of armed conflict reached consensus on the definitions of lawful and unlawful use?

- Has international cooperation against cyber crime been improved?
  - Are international requests for assistance routine and effective?
  - Is information shared internationally quickly enough to have effect?
  - Are the numbers of safe havens for cyber criminals being reduced?
  - Is there international agreement on norms of behaviour that has the effect of modifying the behaviour of nation-states?

- Have the conceptions of cyber security that are currently lacking been internalised within the government?
  - Does procurement policy take account of cyber vulnerabilities?
  - Are there new acquisition rules that incorporate cyber security standards for all hardware?
  - Are cyber security projects funded adequately?

- Has Government taken leadership of the cyber issue?
  - Is there a national strategy in place that identifies roles and responsibilities throughout government and in the private sector? Is it a paper strategy or is it actually being implemented?
  - Does the public understand the scope and nature of the cyber problem?
  - Do they care about it and have they considered how cyber issues impact privacy and civil liberties?
Australia’s Response to the Cyber Challenge

- Has the public’s mindset of cyber security been changed so that good practices are well accepted?
- Is more attention being paid to cyber conflict in military and other national security colleges?
- Has transparency increased, thereby enhancing public debate on the appropriate solution set?
About the Kokoda Foundation

Purpose

The Kokoda Foundation has been established as an independent, not-for-profit think tank to research, and foster innovative thinking on, Australia’s future security challenges. The foundation’s priorities are:

- To conduct quality research on security issues commissioned by public and private sector organisations.
- To foster innovative thinking on Australia’s future security challenges.
- To publish quality papers (The Kokoda Papers) on issues relevant to Australia’s security challenges.
- To develop Security Challenges as the leading refereed journal in the field.
- To encourage and, where appropriate, mentor a new generation of advanced strategic thinkers.
- Encourage research contributions by current and retired senior officials, business people and others with relevant expertise.

Membership

The Kokoda Foundation offers corporate, full and student memberships to those with an interest in Australia’s future security challenges. Membership provides first-release access to the Kokoda Papers and the refereed journal, Security Challenges, and invitations to Foundation events. Membership applications can be obtained by calling +61 2 6295 1555, and downloaded from:

www.kokodafoundation.org
Optimising Australia’s Response to the Cyber Challenge

The Kokoda Foundation embarked on a study of the cyber challenge faced by Australia for two reasons. First, the government’s identification of cyber security as a national security priority; and second, because of concerns that whilst the actions taken by government and some segments of industry are highly laudable, the breadth, scale and growth rate of the threat are such that the current cyber security program is simply not sufficient.

In order to explore these issues, a series of colloquiums, workshops and interviews were conducted with representatives of government departments, industry and other relevant parties. Former US Government officials as well as US and UK industry representatives participated in the colloquiums, along with a large representation of Australians.

This report examines the nature of the cyber challenge confronting Australia. It reviews how government, industry and the public are responding to the threat both individually and collectively from both a domestic and international perspective.