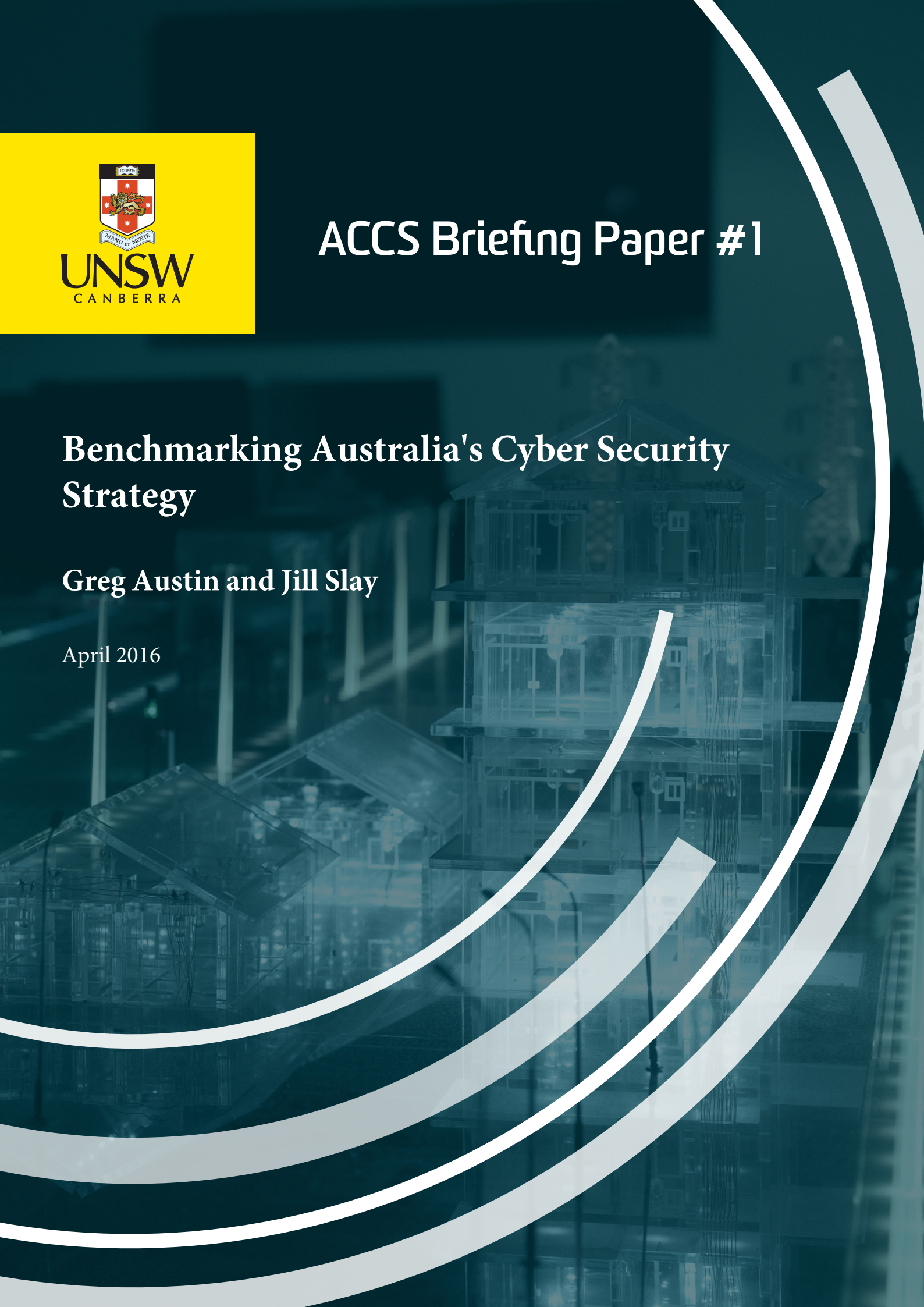


UNSW CANBERRA

ACCS Briefing Paper #1

Benchmarking Australia's Cyber Security Strategy

Greg Austin and Jill Slay

April 2016

UNSW AUSTRALIA

Australian Centre for Cyber Security
UNSW Canberra

BENCHMARKING AUSTRALIA'S CYBER SECURITY STRATEGY:

A FUTURE-LOOKING CHECKLIST

ACCS Briefing Paper No. 1

Greg Austin and Jill Slay

Australian Centre for Cyber Security
University of New South Wales Canberra
19 April 2016

This ACCS Briefing Paper provides a "checklist" of seven key foundations for a sound national strategy for cyber security in Australia. It adopts a benchmarking approach, looking at the United States and United Kingdom as exemplars.

We believe that we should expect to see a reasonable degree of similarity and common elements among the strategies of these three countries given the relative state of their technological and social development in this area of policy. They all participate in a shared global exchange of trade, investment and intellectual property, and they are close allies in cyber security affairs. That said there will also be essential differences based on many other considerations, not least relative wealth, industrial base and political priorities.

The release of the Briefing Paper has been timed to fall just before the release of the new Australian Cyber Security Strategy by the Prime Minister, Malcolm Turnbull, on 21 April 2016. The paper is not intended to pre-empt or foreshadow the detail of the Prime Minister's announcement but rather to offer a set of reference points against which the strategy might be interpreted, not just in the immediate future but also over years to come. Taking the Prime Minister at his word that Australia should become an innovation nation, we expect that the announced cyber security strategy will be subject to regular review and update, and even be subject to significant revision as the need or opportunity arises. This checklist should provide some enduring foundation for reflection on such changes.

The Briefing Paper presents seven over-arching and somewhat general criteria. Each criterion will be covered in a one-page treatment, comprising a prose paragraph, and a "quick look" comparison table of the situation with selected examples of policy and practice from the United States, the United Kingdom and Australia. (The last date of information in the paper was 18 April 2016, several days prior to the release of the new strategy.)

Essential framing considerations for this short briefing are as follows.

- A national cyber security strategy in a liberal democracy and free market economy is not exclusively or even primarily a government-led effort. In many respects, the Australian federal government can only facilitate and inspire within the constraints of tight budgets. Other actors, such a major corporations, industry associations, professional groups, state and local governments, parliamentarians, public service providers, religious bodies, and civil society groups, must play a leading role as well.
- Typically, a national strategy document for cyber security does not capture the totality of the Australian government's policies and practices in the field. Various elements are reflected in other diverse places, including legislation, international treaties and diplomacy, and in various White Papers or strategy documents on defence, defence industry, cyber crime and cyber hygiene.
- Australia sits in a global community of cyber security practice, technologies, policies, public education and research on which it can draw. It does not need to do everything itself from scratch.
- One example of this is our "five eyes" intelligence relationship and the larger set of our strategic relationships with those partners. Another example of this is our openness to enabling factors for cyber security, such as foreign investment, trade and movement of specialists.
- The Australian government has a good news story to tell on some of the enabling factors for cyber security. It may well be in the top ten countries in the world in this

regard. The country's successes in the field have not been as well articulated as they need to be.

- Australia also faces a rapidly evolving and more serious constellation of threats, most of which originate outside the country though some are home-grown and very local (non-national).
- In February 2016, the United States government announced an emergency package of new cyber security measures, including a new spend of $19 billion dollars for FY 2017. The UK has recently announced a five-year spend of 1.9 billion GBP on cyber security measures.
- For five years, the UK government has adopted a practice of annual evaluation of its national cyber security position and strategies, its latest published on 14 April 2016.
- International benchmarks (guidelines) for national cyber security policies in the civil sector have been developed by the European Network and information Security Agency (*An Evaluation Framework*) and by the NATO Cooperative Cyber Defence Centre of Excellence (*Framework Manual*). These inform the Briefing Paper.

This Briefing Paper has also referenced public submissions to the current Cyber Security Review which can be accessed, along with other resources, on the government's website.

This Briefing Note will serve as the foundation for a one-day workshop on the new Australian cyber security strategy to be held later this year and for a subsequent ACCS Discussion Paper based on the Workshop.

WHAT IS CYBER SECURITY?

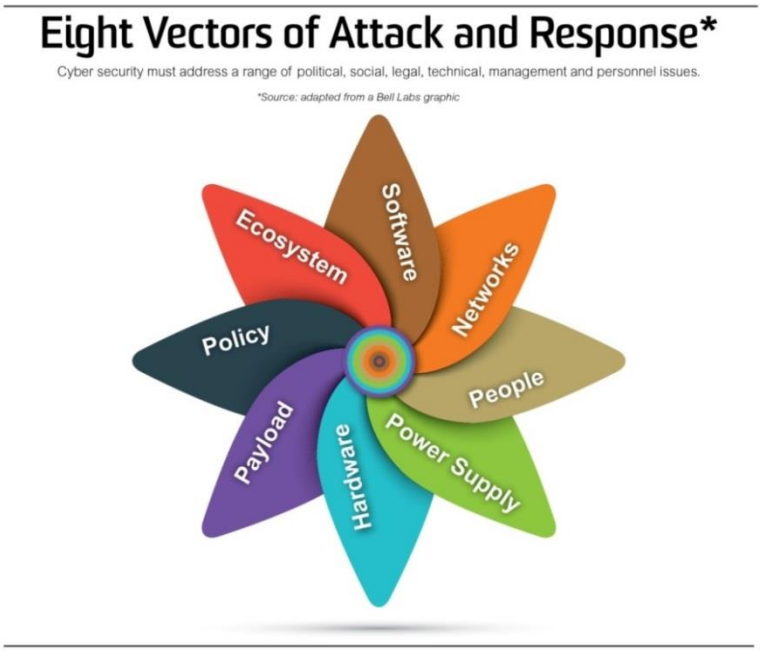
The term "cyber security" covers a multitude of quite diverse considerations. Each country, and even actors within one country, will focus on a different combination of these considerations because they will have different organisational priorities and quite distinct economic and security potentials.

In broad terms, "cyber security" has at least eight "ingredients" or foundation elements, some of which are narrowly technical (but which all involve human input and institutions) and others of which are simultaneously technical but deeply dependent on non-technical inputs. One view of these ingredients is captured in Figure 1 on the next page which describes them as vectors of attack and response.

This graphic in Figure 1 is adapted from an approach developed by engineers in Bell Labs to address problems of protection of information and information systems at the enterprise level and to protect enterprise connectivity. The Bell Labs concept and our adapted graphic provide a very useful departure point for broadening public understanding of what shapes security in cyber space. At the same time, even this approach does not do justice to wider institutional, political, legal and social aspects of the problem set. At the national level, all strategy and planning for cyber security depend on the institutional, political, legal and social environment as much as they do on engineering, systems management or capability-based approaches such as those implicit in the Bell Labs concept, which was developed almost a decade ago.

Box 1 on the next page sets out the checklist on which the Briefing Paper is structured.

Figure 1: A Cyber Security Model



Box 1: The Checklist

1. Consistent articulation of the different domains of cyber security (crime, harassment and bullying, critical infrastructure resilience, espionage, warfare); of the many dimensions of cyber security (technical, human, social and legal); and how different sections of the society must bear differentiated responsibilities.

2. Consistent and comprehensive articulation of the threat environment and variegated response options.

3. A comprehensive suite of governmental, cross-sector, private-public, professional and civic organisations active in cyber security.

4. National consensus on where to draw the line between sovereign capabilities and the global communities of practice (including R&D)

5. Effective monitoring of business and economic threats and rapid response capabilities at the enterprise level, including large corporations and SMEs.

6. Nation-wide preparedness for the unlikely but credible threat of an extreme cyber emergency affecting the civil economy or national security interests (including international aspects).

7. Effective response capabilities for social threats (crimes) against individuals, including children and other vulnerable groups.

1. ***Consistent articulation of the different domains of cyber security (crime, harassment and bullying, critical infrastructure resilience, espionage, warfare); of the many dimensions of cyber security (technical, human, social and legal); and how different sections of the society must bear differentiated responsibilities.***

The best national strategies are those that are a combination of government policies, voluntary standards, legislation, enforcement, private sector leadership, civil society mobilisation and individual activity. In such cases, there are always a number of distinct policy documents from the different actors, often staking out contradictory views. The multi-actor "set" of national strategies will identify quite distinct objectives, enabling stakeholders to differentiate between the different types of threat and security responses available in quite different areas of social, political and economic activity. National cyber security strategies should have an array of objectives that differ according to the problem (crime, espionage, critical infrastructure resilience, harassment, or war), the main actors involved (such as national, state or local governments, police, public health, national emergency services or privacy protection agencies), and the value of the information being protected within each of those problem sets or actor groups. In the NATO Framework Manual (pp. 34-43) mentioned above, Melissa Hathaway and Alexander Klimburg identify five dilemmas in national cyber security policy:

- Economic stimulation vs. national security
- Public sector vs private sector
- Infrastructure modernisation vs critical infrastructure protection.
- Data protection vs information sharing
- Political stability vs freedom of expression.

Their intent in discussing these dilemmas is to underscore the difficulty in any country of arriving at a clear understanding of what national cyber security priorities should be. They also highlight the degree of political contest that will underpin any set of national strategies.

Table 1: Selected Data Points on Differentiation of Types of Cyber Security Threats: the Example of Cyber Crime as a Distinct Policy Priority

United States	United Kingdom	Australia
In February 2016, the United States announced that "The Department of Justice, including the Federal Bureau of Investigation, is increasing funding for cybersecurity-related activities by more than 23 percent to improve their capabilities to identify, disrupt, and apprehend malicious cyber actors". It singled out identity theft as the "fastest growing crime in America". In April 2011, the White House a specific policy on "Trusted Identities in Cyberspace", to prevent this form of crime.	The 2016 Cyber Security Strategy Annual Report contains many references to different types of cyber crime and granular analysis of it. The report states that "The Government has invested in law enforcement capabilities at national, regional and local level to ensure that police forces have the capacity to deal with the increasing level and sophistication of online crime." It also reports that in 2015, the Office for National Statistics piloted new cyber questions for its regular Crime Survey.	In April 2015, the Australian Information Industry Association called for greater policy attention to cyber crime, especially through greater emphasis on its increasing sophistication. The ACSC 2015 Threat report identifies this as a problem, but has little granular analysis. In April 2105, an independent evaluation on terrorist financing found a lack of engagement by police forces in most jurisdictions in Australia with using high quality nationally available (cyber) surveillance data.

2. *Consistent and comprehensive articulation of the threat environment and variegated response options.*

Cyber security does not exist for its own sake, but to protect people, enterprises and governments from a wide variety of serious threats that will be place-specific and time-specific. Threat assessment, tracking and reporting is a recognised priority in almost all jurisdictions where national cyber security strategies exist, but the style, scope and consistency of this threat assessment can be quite varied. Various national level assessments by government compete with private sector assessments from around the world. In many smaller countries, there is a reliance on governmental assessments coming from the United States, Europe or regional organisations (such as the African Union or the Organisation of Islamic Cooperation). Private sector threat assessments from leading ICT corporations, such as Microsoft, McAfee, Kaspersky Lab, Symantec and Verizon, do not report according to a shared model and have a media prominence that interferes with government messaging. In the more coherent national strategies, especially the United States, threat assessments are the departure point of all policy settings. The NATO Framework Manual noted that "with no formal review mechanism in place", many nation cyber security strategies "may become irrelevant or unable to provide guidance when facing a new type of cyber challenge". There is clear bias in most countries away from comprehensive threat analysis in open source documents in favour of risk-based approaches.

Table 2: Selected Data Points on Consistent Articulation of Cyber Security Threats

United States	United Kingdom	Australia
Each year, leading figures in the United States intelligence, security and justice community report to Congress in public on cyber threats in a consistent, comprehensive and detailed fashion. In March 2016, President Obama reported to Congress: "Significant malicious cyber-enabled activities" from outside the country "continue to pose an unusual and extraordinary threat to the national security, foreign policy, and economy of the United States". In December 2015, the passage of the Cybersecurity Act made it "easier for private companies to share cyber threat information with each other and the Government". In February 2016, the government announced it was setting up a resilience centre for critical infrastructure operators to understand threats.	In 2011, the UK committed to annual reviews of the effectiveness of its cyber security policies, which address in part a threat assessment. The 2016 Cyber Security Strategy Annual Report indicates a variety of consistent threat assessment venues and formats. It notes that the "Centre for Cyber Assessment provides assessments of threats and vulnerabilities to more than 40 government departments and agencies". It also notes that "Cyber risk reviews of the UK's CNI have increased government, regulator and industry understanding of the risks and have led to further work on mitigations, supported by bespoke guidance." But, a 2014 survey of FTSE 350 companies revealed "less than a third (30%) of boards received high level cyber security intelligence from their Chief Information Officer or Head of Security".	In 2015, ACSC issued Australia's first comprehensive and unclassified Threat Report. It noted that "Australia has not yet been subjected to any activities that could be considered a cyber attack" (which it defined as an attack "seriously compromising national security, stability or prosperity".) It also assessed that "Robust cyber defences will continue to allow a high degree of confidence in network and information security." In 2015, its inaugural survey of cyber threats to Australian businesses, with fairly basic questions about frequency and type of attack, concluded that "Australian businesses are yet to be convinced about the benefit of reporting". The threat actors of most concern to Australian businesses (p. 23) in the survey were canvassed only in the broadest of terms in the ACSC's 2015 Threat Report.

3. A comprehensive suite of governmental, cross-sector, private-public, professional and civic organisations active in cyber security.

Most governments explicitly accept that cyber security depends on widespread collaboration among key stakeholders, both at home and internationally. Yet not all have followed through on that commitment with comparable institutional and social development. The NATO *Framework Manual* (pp. 94-107) makes a useful distinction between three approaches which represent evolutionary stages in development of national cyber security strategies from this point of view: whole of government, whole of nation, and whole of systems. The meaning of the first two terms is quite obvious. A good example of the whole of nation approach is the creation in 2011 in the Netherlands of a Cyber Security Council (CSR -- for its name in Dutch). It is a national and strategic advisory body for the government and the country as whole. It comprises "highly-placed representatives in scientific, public and private organisations". Its functions also include "advising the government on the implementation and development of the National Cyber Security Strategy II", "contributing to research in the scope of the Dutch Cyber Security Research Agenda", and "deploying CSR members during large-scale cyber incidents. The "whole of system" approach is one that complements other policies by giving special attention to the international environment in which a country must establish its cyber security strategies and ensure defence and security against cyber threats. Countries which effectively pursue a whole of system approach are normally those with the most highly developed whole of nation approach and whole of government approach. Small countries can benefit from the global public goods created by larger states with a committed internationalist vision of cyber security.

Table 3: Selected Data Points on a Comprehensive Suite of Relevant Organisations

United States	United Kingdom	Australia
The USA pursues a whole of systems approach. In 2011, alongside a myriad of other cyber security strategies, the USA published its *International Strategy for Cyberspace*. Its private sector actors are now the mainstay of ICANN, and the United States has played a leadership role in most international initiatives or organisations with a cyber remit, since the early 1990s. These include the Roma-Lyon High Tech Crime sub-group of the G7 (G8). APEC has a highly developed framework for cyber security cooperation but the USA was for some years not as committed as Australia to cyber security cooperation in this forum. The USA is the world leader in NGO mobilisation around cyber security.	The United Kingdom pursues a whole of systems approach. In 2011, it launched the London process, which led to a series of four international conferences on international collaboration for freedom of the internet. This activity built off the strong domestic foundations in place around cyber threats to critical infrastructure protection. It also leveraged many civil sector organisations, such as the Information Assurance Advisory Council, a not for profit research organisation that serves as a forum for all stakeholders. Like the United States, the UK has seen private NGOs spring up around the issue of online child safety. These include the Coalition on Internet Safety founded in1999.	Australia pursues a whole of systems approach, but with visible institutional gaps relative to the USA or the UK in terms of a whole of nation approach. On the international front, Australia has been active in various cybersecurity forums, not least the UN Group of Governmental Experts working on voluntary cyber norms. In 2015, the Defence Department issued a privately authored report under the title, "Time for a Whole of Nation Approach to Cyber Security". It concluded that the government "has not provided the environment that enables it to partner with and leverage the skills and capabilities of other areas of the Australian and international communities".

4. National consensus on where to draw the line between sovereign capabilities for cyber security and the global communities of practice (including R&D)

The globalisation of the ICT sector and of cyberspace itself has brought into question each country's pre-established policies on the balance to be struck between desirable cross-border trade and investment in strategic goods and the non-desirable. New variations on the theme of sovereign capability have emerged around the need to contain unchecked cyber surveillance by foreign states and loss of privacy to the big "information utilities", the need to work harder to shield nationally sensitive information from disclosure and cyber espionage, and even the need for additional limitations on scientific exchange between researchers working on matters like cryptography. The global deficit in skilled professionals in some areas of cyber security has added a new urgency to resolving some of the contradictions about sovereign capability. At the heart of the challenges have been the five dilemmas of national cyber security policy elucidated by Hathaway and Klimburg and mentioned under Criterion #1 above. In most countries, these dilemmas have been resolved by intuitive, incremental and largely irrational policy making. The United States and the United Kingdom stand out most sharply as global leader in these debates. The best elaboration of the balance to be struck between sovereign capability and global communities of practice is the 2011 White House International Strategy for Cyberspace, and it comes down heavily in favour of global participation because, it says, only this path promotes continued economic prosperity for all and global stability. It is relative silent on the very sharp restrictions the United States imposes in narrow areas of technology and expertise to maintain its sovereign capabilities. The relationship that countries have with China encapsulates rather well the character of this criterion for an effective national strategy for cyber security.

Table 4: Selected Data Points on the Dilemmas of Sovereign Capability with Regard to China

United States	United Kingdom	Australia
The USA has allowed an explosion of Chinese investment in its ICT sector beginning in 2014, while continuing to place national security limits on where Chinese corporations such as Huawei can invest. Huawei profits in the USA continued to grow in 2015 in spite of a turn down in business from the big U.S. telecoms companies. USA has an aggressive policy of skilled migration in the ICT sector, including from China, while carefully developing a sovereign capability among U.S. and Allied citizens. The USA has led an unprecedented and robust campaign to limit economic and commercial damage from China's cyber espionage, what the USA has called a "national emergency".	The UK has stridently and coherently articulated the need to maintain sovereign capabilities in cyber space, in a way that is quite different from the USA, where the stance is simply taken as a given. The UK shares almost identical concerns with the USA about the needs in this area but has inherited and continued a deep engagement with Huawei. In March 2015, a UK-mandated oversight board reported that "any risks to UK national security from Huawei's involvement in the UK's critical networks have been sufficiently mitigated". The UK and China signed an agreement not to undertake commercial espionage, even as officials described China's cyber espionage as endemic.	The public debate in Australia about sovereign capability has gained more prominence in respect of submarine and naval ship-building than for cyberspace issues. Australia has followed the U.S. lead on Huawei and suspicions about its links to Chinese cyber espionage by not allowing it to bid for the contract on the National Broadband Network and consideration of other measures. Private sector interests have articulated a need for an expanded national skills base, but have not drawn the "sovereign"/security aspect in detail. Like the UK, Australia participates with China in programs for S&T exchange on cyber security related issues and promotes work visas for Chinese researchers.

5. *Effective monitoring of business and economic threats and rapid response capabilities at the enterprise level, including large corporations and SMEs.*

The monitoring and analysis of business and economic threats to enterprises in cyber space have many aspects. At one level, there are the technical intrusions themselves, which impose short term demands for terminating the threat. On another level, there are cumulative dollar costs to a single enterprise of the totality of the attacks it might suffer over several years. In some cases, there are potential liability obligations on the enterprise that might flow from data breaches severely affecting the rights of third parties. At an even higher level, there are national level considerations that go to understanding of a possible threat to an entire sector (such as banking, civil aviation or transport), to national economic prosperity or national security. All three aspects of enterprise-based threat monitoring analysis and rapid response therefore need to engage with actors external to the firm to some degree, and often in foreign countries. In all jurisdictions, as a broad generalisation, these processes of collaboration outside the enterprise are weakly developed in spite of individual leading corporations being adept at it. ENISA has identified improvements in this area of activity as important for protection of critical national infrastructure in cyberspace (pp. 29, 32). The NATO Framework Manual described the efforts that had been made in member countries, and assessed that "While not robust, these initiatives are trying to establish bi-directional information sharing architectures to accelerate better understanding or situation awareness about how industry or the nation overall is being targeted" (p. 40). This activity confronts one of the five dilemmas identified by Hathaway and Klimburg, the tension between an enterprise needing to keep its business data confidential while having a competing interest in maximising cyber security outcomes for itself, its peers and the country as whole.

Table 5: Selected Data Points on Responses to Business and Economic Threats: The Example of Incident Reporting and Sharing of Information

United States	United Kingdom	Australia
In February 2015, the President signed an Executive Order on promoting information sharing for cyber security. There are many organisations mobilised round this task from national government departments (NSA, FBI, Justice, and DHS), state governments with their own frameworks and private sector networks, especially the "ISACs". Even so, in February 2016, the Administration announced that in several months it would "publicly release a policy for national cyber incident coordination … so that government agencies and the private sector can communicate effectively and provide an appropriate and consistent level of response".	In 2016, the UK reported that it had "10 Regional Information Sharing Groups and over 1750 organisations in CISP, the Cyber Security Information Sharing Partnership for Industry & Government". CISP was set up in 2013 and is now managed by UK-CERT. To better prosecute cyber crime through international information sharing on incidents, the UK's Revenue and Customs agency signed an MoU with the U.S. Internal Revenue Service. International investment banks based in London operate their own information sharing mechanism and work with UK agencies.	CERT Australia is the main focal point for businesses to report cyber incidents, and has partnerships with 500 firms. The Australian Information Security Association reported in 2015 its survey results that the "top challenges" in cyber security are "poor information sharing and failure at the executive level to appreciate security risks". The telecommunications sector advised the government in 2015 that it "ought to consider creating a legal framework of the kind proposed in the US Cyber Intelligence Sharing and Protection Act" to eliminate enterprise liability to third parties from sharing their information with authorities in good faith.

6. *Nation-wide preparedness for the unlikely but credible threat of an extreme cyber emergency affecting the civil economy or national security interests (including international aspects).*

Specialists and governments around the world are almost unanimous that a catastrophic cyber emergency is highly unlikely in peacetime but they cannot agree on what priority to accord planning for one in national cyber security strategies. A number of governments, especially the United States and Estonia, view the threat as credible and have accorded such a possibility a high priority in their planning. This approach conforms to the traditional policy line that while outright war with major powers, like China and Russia, is highly unlikely, it is still essential to have defence capabilities in place, as well as mobilisation plans, for the eventuality. However, the need to plan for extreme cyber emergencies is not only driven by the familiar contingency dictates of national defence policy, but the unique characteristics of cyber space, diverse vectors of attack, or system failure within advanced systems. The NATO Framework Manual observes that governments "recognise that a disruption in one infrastructure can easily propagate into other infrastructures" with catastrophic consequences. It also observes that highly developed resilience strategies for extreme cyber emergencies are an essential part of military deterrence in the cyber age (p.82). Some leading private sector organisations also accord a high priority to planning for extreme cyber emergencies. In 2013, a global survey by the World Federation of Exchanges (WFE) and the International Organization of Securities Commissions (IOSCO) found that 89 percent of respondent exchanges considered that cyber crime in securities markets can be considered a systemic risk. It continued to develop policy responses and in November 2015 advised its members to plan for "extreme but plausible scenarios" (p. 2).

Table 6: Selected Data Points on Preparedness for an Extreme Cyber Emergency

United States	United Kingdom	Australia
Since 2006, the USA has conducted biennial exercises in the Cyber Storm series to test responses in national cyber emergency situations. Idaho National Laboratory conducts research on nation resilience in the face of "catastrophic and potentially cascading events that will likely require substantial time to assess, respond to, and recover from." In 2010, Sandia National Laboratory warned of seven structural defects in U.S. decision-making that would undermine its resilience in an extreme cyber emergency. In 2011, President signed PPD 8 on national emergency preparedness, including for nationally significant cyber attack.	The UK sees responsibility for defending critical national infrastructure as sitting "firmly with industry", while the "government works closely with them to provide advice, assurance and expertise", including through "joint exercises to improve preparedness". "On average, CERT-UK supports three exercises per month to test cyber resilience and response" (p.23). The Bank of England has led two "Waking Shark" table top exercises in 2011 and 2013, to test the financial sector against an extreme and concerted cyber attack by a hostile country. In 2016, the UK and USA will partner in an exercise to test a terrorist cyber-enabled attack on a nuclear power station.	ACSC's 2015 Threat Report says extreme cyber attack is unlikely "outside a period of significant heightened tension or escalation to conflict with another country". In 2011, ANZUS partners agreed that the treaty could be invoked in the event of a serious cyber attack. The government's 2015 resilience strategy for critical infrastructure mentions cyber threats in general terms. In 2013, ASPI assessed that "Australia's cyber policy looks disjointed and lacking in detail". Australia has participated in an Asia Pacific cyber exercise and the U.S. Cyber Storm series. In 2013, an officer of the Commonwealth Bank identified 7 extreme cyber scenarios to focus attention on this problem set.

7. Effective response capabilities for social threats (crimes) against individuals, including children and other vulnerable groups.

The NATO Framework Manual reviewing national strategies for cyber security and published in 2012, reveals little attention by states to child safety online as part of the cyber security problem set. The situation has changed dramatically in the intervening four years. The take-off date globally was probably around 2010 or 2011 when the protection of children in cyber space was understood as a much more serious problem than the long-standing and ghastly practices of internet-based child pornography. A 2011 UNICEF study paints the poor state of affairs at that time quite well, while noting that certain industrialised countries, especially in the European Union, were well ahead. The United States had been the pacesetter, setting up a Task Force in 1998 on Internet Crimes against Children. The 2009 Australian cyber security strategy mentions child safety online as a very important policy agenda but did not see it as part of the cyber security strategy's focus. It saw the role of the strategy as "primarily concerned with the availability, integrity and confidentiality of Australia's ICT" (p. v). The International Telecommunications Union has provided some guidance on national strategy development in this sphere (pp. 71-72), which emphasise the obligation of states to create and fund the appropriate law and justice mechanism, as well as social support services. The transition in play now is from seeing cyber bullying as harassment to seeing it as a crime, with ever more severe penalties.

Table 7: Selected Data Points on Responses to Social Threats to Individuals: The Case of Crimes against Children Online

United States	United Kingdom	Australia
Early milestones included the Child Online Protection Act (COPA) of 1998, the 1998 Children's Online Privacy Protection Act (COPPA), the 2000 report of a Commission set up by the COP Act, and a 2002 research report on "Youth, Pornography, and the Internet" by the Computer Science and Telecommunications Board National Research Council (2002). In 2008, a Task Force set up by the 52 Attorneys General (state, territory and federal) made recommendations on the potential of technologies to offer enhanced protections for children online. In 2011, the U.S. CERT took a more prominent position on protection of children online, and protection of data and systems of other users while children are on line.	In 2010, the government set up the UK Council for Child Internet Safety (UKCCIS), which by 2016 had become a "group of more than 200 organisations drawn from across government, industry, law, academia and charity sectors". It currently has five working groups. The National Crime Agency (NCA) has a command called the Child Exploitation and Online Protection Centre (CEOP), first established in 2006 and taken over by the NCA in 2013. In December 2015, the government announced its plan to "put in place strengthened measures to protect children from harm online - including cyber bullying, pornography and the risk of radicalisation". The UK has moved to stiffen penalties, including imprisonment for up to two years, for cyber bullying.	In 2008, the government set up a Cybersafety program ($125.8 million over four years) "to combat online risks and help parents and educators protect children from inappropriate material". In 2010, the parliament set up a Joint Select Committee on Cyber Safety that released a report on children in 2011. In March 2015, the parliament passed the Enhancing Online Safety for Children Act 2015 setting up the office of the Children's e-Safety Commissioner. The Act also provided for a complaints system to get harmful material down fast from large social media sites. In January 2015, the Australian Council on Children and the Media critiqued the draft bill as too narrow for its exclusive focus on cyber bullying. The Senate is now conducting a new inquiry on harm done to children by pornography on the internet.

ABOUT ACCS

The Australian Centre for Cyber Security (ACCS) at the University of New South Wales Canberra is two things. First, it is a focal point for 60 scholars from various faculties across UNSW who conduct research work on different aspects of cyber security. Second, it is a unit based in Canberra at the Defence Force Academy that provides both advanced research as well as undergraduate and graduate education on cyber security. ACCS brings together the biggest concentration of research and tertiary education for the study of cyber security in any single university in the Southern hemisphere. A number of ACCS scholars, in areas ranging from information technology and engineering to law and politics, have significant international reputations for their work.

https://www.unsw.adfa.edu.au/australian-centre-for-cyber-security/

Dr Greg Austin is a Professor in the Australian Centre for Cyber Security. He also serves as a Professorial Fellow at the East West Institute, where as Vice President from 2006-2011 working from London and Brussels he helped set up and lead its Worldwide Cyber Security Initiative. Greg is a co-chair of the EastWest working group on Measures of Restraint in Cyber Armaments. He has held senior posts in the International Crisis Group and the Foreign Policy Centre (London). Other assignments include service in government, defence intelligence, academia and journalism. Greg has collaborated with the NATO Cooperative Cyber Defence Centre of Excellence in Tallinn, including in its recently published book, *Int*ernational Cyber Norms: Legal, Policy & Industry Perspectives. Greg is the author of several books on China's strategic policy, including *China's Ocean Frontier* (1998) and his most recent book, *Cyber Policy in China* (Wiley 2014). This book offers the first comprehensive analysis (military, economic and political) of China's leadership responses to the information society. It explores the dilemmas facing Chinese politicians as they try to marry the development of an information economy with old ways of governing their people and conducting international relations. The book concludes that unless China's ruling party adapts more aggressively to the defining realities of power and social organization in the information age, the 'China cyber dream' is unlikely to become a reality. Greg has a Ph D in International Relations and a Master's degree in international law.

Professor Jill Slay AM is the Director of the Australian Centre for Cyber Security. Professor Slay's research has focused on Forensic Computing for the last ten years although she has a well-established international research reputation in a range of aspects of cyber security including critical infrastructure protection and cyber terrorism. With a variety of collaborators, she has instigated cross-disciplinary research that draws on social science, anthropology, law, drugs and crime, police and justice studies, as well as systems and communications engineering and IT, to achieve its aims. She advises industry and government on strategy and policy in this research domain. Jill has published one book and more than 120 refereed book chapters, journal articles or research papers in forensic computing, information assurance, critical infrastructure protection, complex systems and education. She has been awarded approximately AUD2 million in grant funding since 2005. Jill is a Fellow of the International Information Systems Security Certification Consortium (ISC2) and a member of its Board. She was made a member of the Order of Australia (AM) in 2011 for her service to the information technology industry through contributions in the areas of forensic computer science, security, protection of infrastructure and cyber-terrorism.