SPECIAL REPORT

ASPI

July 2013

ASPI AUSTRALIAN STRATEGIC POLICY INSTITUTE

INTERNATIONAL CYBER POLICY CENTRE

The emerging agenda for cybersecurity

by Peter Jennings and Tobias Feakin

Introduction

Cybersecurity is rapidly emerging as a high-priority policy challenge for the Australian Government. The National Security Strategy released in January 2013 listed 'malicious cyber activity' as the third of seven 'key national security risks' and called for closer partnerships with the business community to develop a more effective response. Former Prime Minister Julia Gillard visited the Defence Signals Directorate (DSD) headquarters in Canberra following the release of the strategy to announce the creation of the Australian Cyber Security Centre (ACSC), which will co-locate cyber operational capabilities from a number of agencies. DSD noted that in 2011–12 there were more than 400 cyber incidents against government systems, requiring a significant response by its Cyber Security Operations Centre, and that 5.4 million Australians were victims of cybercrime in 2012 at an estimated cost to the economy of $1.65 billion.[1]

The rise of cybersecurity as an Australian policy priority reflects growing international concern about the impact of malicious cyberactivity. In February 2013, US President Obama issued an executive order on improving critical infrastructure cybersecurity, referring to cyber as 'one of the most serious national security challenges we must confront'. The order sets out a detailed plan to rapidly create a strengthened government and private sector approach to protecting critical infrastructure from cyberattack.[2] Recent detailed accounts in the *New York Times* and from private sector analysis of Chinese cyberattacks point to unprecedented public concern about malicious cyberactivity.[3] This has impacts on Australia too, as cybersecurity finds its way onto agendas for discussions with our allies and regional partners.

Notwithstanding recent government policy announcements, this paper argues that significantly more needs to be done to ensure that Australia has the right policies in place to manage cybersecurity risk. The paper discusses the organisational problems that have slowed Australia's work to develop a simple but effective cyber policy, and contrasts our experience with steps taken by our closest allies, the US and UK. It then details ASPI's perspective on the emerging agenda for cybersecurity in Australia, recommending steps that the government should take to develop a clear policy framework. Much of this work will need to be done quickly after the 2013 federal election so that Australia can play an influential role in shaping a global approach to cybersecurity.

The Australian organisational framework

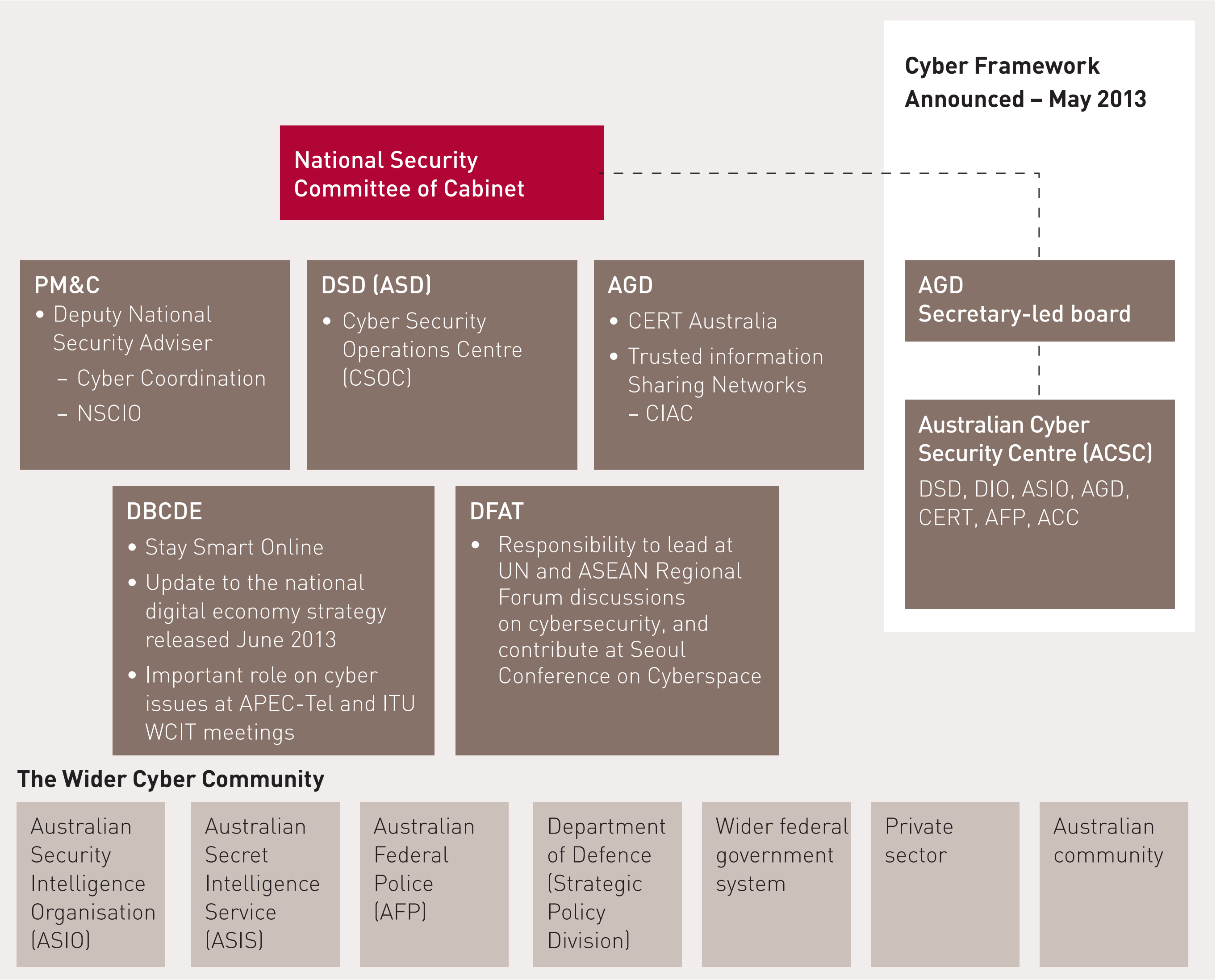
One of the problems inherent in cybersecurity is the sheer number of government and private sector entities that have a legitimate interest in the field. This adds enormously to the complexity of cyber policy development. The Australian Government's 2009 Cyber Security Strategy lists nine agencies, units or committees with critical cybersecurity responsibilities, but the number's really much larger and growing.[4] The *Intelligence Services Act 2001*, which governs DSD's operations, gives the agency responsibility for information security across all government operations, not simply Defence. DSD's Cyber Security Operations Centre was established in 2009 to create a single gathering and reporting point for information on detecting and defeating cyberthreats. Within the Attorney-General's Department (AGD), a computer emergency response team was rebranded in 2010 as CERT Australia, to provide a single point of contact on cybersecurity information for Australian businesses and individuals.

In January 2013, the Prime Minister announced the creation of the ACSC, which, she said:

> will be the hub of the government's cyber security efforts. It will include, in one place, cyber security operational capabilities from the Defence Signals Directorate, Defence Intelligence Organisation, Australian Security Intelligence Organisation, the Attorney-General's Department's Computer Emergency Response Team Australia, Australian Federal Police and the Australian Crime Commission.

In May 2013, the Prime Minister announced that DSD was to be renamed the Australian Signals Directorate (ASD). The new name was said to more accurately reflect the agency's national, cross-departmental role, but the Prime Minister hastened to add that there would be no change to its functions, powers or accountability structures.[5]

Table 1: Current and planned cybersecurity policy machinery



Cyber Framework Announced – May 2013

National Security Committee of Cabinet

PM&C
- Deputy National Security Adviser
  - Cyber Coordination
  - NSCIO

DSD (ASD)
- Cyber Security Operations Centre (CSOC)

AGD
- CERT Australia
- Trusted information Sharing Networks – CIAC

AGD Secretary-led board

Australian Cyber Security Centre (ACSC)
DSD, DIO, ASIO, AGD, CERT, AFP, ACC

DBCDE
- Stay Smart Online
- Update to the national digital economy strategy released June 2013
- Important role on cyber issues at APEC-Tel and ITU WCIT meetings

DFAT
- Responsibility to lead at UN and ASEAN Regional Forum discussions on cybersecurity, and contribute at Seoul Conference on Cyberspace

The Wider Cyber Community

Australian Security Intelligence Organisation (ASIO)

Australian Secret Intelligence Service (ASIS)

Australian Federal Police (AFP)

Department of Defence (Strategic Policy Division)

Wider federal government system

Private sector

Australian community

Who ‘owns’ cyber policy?

These measures point to a consolidation of cyber functions, particularly at the operational level, where information technology specialists detect cyber intrusions and deploy countermeasures. The bulk of government investment in strengthening cyber capability has happened at that highly technical level. The ACSC also aims to build stronger, practically focused links with the private sector. The goal to have the new stand-alone facility operating by the end of 2013 looks unlikely to be achieved, but the focus on practical technical matters is one important part of a holistic policy response. A major criticism of the formation of the ACSC was that there was no new finance put in place for the centre. This means that it will be built on the resources that each department brings with it, which wouldn’t be a model encouraging true cooperation between agencies. Having a central pool of funds for the ACSC would give impetus for each organisation to further their collaborative work rather than worrying about fulfilling their own budgetary requirements.

Sadly, the story is much less positive at the level where governments, agencies and businesses develop cyber policy—the handling strategies needed to support good-quality decision-making on cyber matters. As cyber lifts in national priority, the need is to ensure that our policy development capacities also increase. In the past few years, however, responsibility for cyber policy has been shifted between no fewer than three departments.

AGD originally had responsibility for what Canberra calls ‘whole-of-government’ coordination on cybersecurity policy. The department produced the 2009 Cyber Security Strategy, and according to that document ran the Cyber Security Policy and Coordination Committee (responsible for policy development for the government).

In April 2009, the position of National Security Chief Information Officer (NSCIO), double-hatted as the Cyber Policy Coordinator, was created in the Department of the Prime Minister and Cabinet (PM&C). A tug-of-war began between AGD and PM&C over which department had the lead on cybersecurity.

In June 2011, PM&C announced that its Cyber Policy Coordinator would develop a Cyber White Paper. White papers are iconic documents, and this one was planned to ‘for the first time bring together and describe the important relationships in the cyber environment between our social well-being, our economic prosperity and our broader national interests.’[6]

With such a grand objective for the Prime Minister’s department, it was unlikely that AGD would win the tug-of-war. On 14 December 2011, responsibility was handed over to PM&C.[7]

The Cyber White Paper, originally promised for release in the first half of 2012, experienced a series of delays. Responsibility for its production was quietly transferred to the Department of Broadband, Communications and the Digital Economy (DBCDE). There, the focus of the white paper was said to be ‘broadened’ away from cybersecurity. Prime Minister Gillard told a conference in October 2012 that ‘we should be broadening that out so it is more a digital white paper and helps us capture some of the more profound and longer term issues that have been brought to the table.’[8]

What was ultimately released on 12 June 2013 was not a Digital Economy White Paper but a more limited statement described as an ‘update to the national digital economy strategy’ released in 2011. A number of peak bodies were approached to provide submissions on what cyber security issues the document should address. The final product is however, very disappointing. A seven page chapter on ‘safety and security’ does little more than to list a range of current initiatives from countering cyber bullying to a number of outreach activities. The document indicates that the government plans to:

- release the Digital Citizenship Best Practice Principles in the second half of 2013
- develop and promote cybersecurity guidance material designed for small- to medium-sized enterprises
- release a national plan to combat cybercrime in mid-2013
- work with the international community to develop international rules and norms as represented by the United Nations Charter and other international laws.[9]

Readers can be forgiven for thinking that this was precisely what the Cyber White Paper was intended to do. What has been delivered instead is the same piecemeal aggregation of various cyber-related initiatives, and the promise but no delivery of yet more 'principles', 'guidance' and 'plans'. The demise of the Cyber White Paper was a messy business, and its replacement has produced little clarity.

Within PM&C, the position of National Security Chief Information Officer and Cyber Policy Coordinator was abandoned as a stand-alone appointment. It's been added to the responsibilities of the Deputy National Security Adviser, who also has substantial responsibilities for counterterrorism coordination and emergency management.[10]

The most recent organisational reshuffles in cyber policy were announced in May in the 2013 Defence White Paper with the renaming of DSD to the Australian Signals Directorate, and in the announcement of the creation of the ACSC in January 2013. The white paper said that 'the Centre will be overseen by a Board, led by the Secretary of the Attorney-General's Department, with a mandate to report regularly to the National Security Committee of Cabinet.'[11]

In effect, we've returned to the situation that applied in 2009: AGD has the lead in reporting cybersecurity issues to government, this time through a board rather than through the Cyber Security Policy and Coordination Committee. Most concerning, though, is that the drive for a Cyber White Paper has been lost and the skill base for policy work in the major departments has been eroded through constant changes of role. The new ACSC will focus on operational matters rather than on policy, so AGD will report to government on cyber incidents rather than on shaping policy choices.

The answer to the question 'Who owns cyber policy?' is that no department or agency has a strong grasp on that area right now. It's not surprising that the Business Council of Australia's submission on the Digital Economy White Paper rather sharply said that the white paper should 'present a coherent government strategy to deal with cyber security, drawing together multiple existing initiatives'.[12]

The US experience

In the US under the Bush administration, a separate office in the White House was established in 2001 to handle its coordination of cybersecurity matters, led by a special adviser for cybersecurity. This position was not maintained from 2003 to 2008, when the most senior official in government charged with coordinating cybersecurity was placed within the Department of Homeland Security. The US has had many false starts in trying to bring together the various strands of its work on cybersecurity during the 2000s, and it has taken most of that decade to create the impetus behind policymakers to begin to formulate a relatively unified position on the issues.

In 2009, President Obama commissioned a 60-day review of cybersecurity, and one of the key recommendations was to establish a permanent position in charge of cybersecurity. This position of cybersecurity coordinator, (often referred to as the 'cyber czar'), with the rank of special adviser is part of the White House staff and reports to the Deputy National Security Advisor.[13] The role was filled by Howard Schmidt until May 2012, when Michael Daniel took over. Although part of the White House national security team, the cyber czar also consults with the President's top economic advisers and has direct access to the President.

The cyber czar has a coordinating role involving all of the defence and civilian agencies with a stake in cyber matters, including the Department of Defense, the National Security Agency, the Federal Bureau of Investigation, the State Department, the US Computer Emergency Readiness Team and the Department of Homeland Security. The czar implements policies across all of the organisations involved, which is no easy task. The position doesn't carry any direct budgetary power for these areas, and has been criticised for holding large-scale responsibility but no real authority.[14]

The coordinator's role isn't confined to the government sector. It also carries responsibilities for liaising with the private sector to help business manage security risks.

Obama's February 2013 executive order on improving critical infrastructure cybersecurity has been welcomed as a major policy development. It came at a time when the US was struggling to create sufficiently mature information-sharing machinery within its critical infrastructure networks that could increase cyber resilience. The order, which doesn't have the same power as law, did three things. First, it directed federal authorities to improve information sharing on cyberthreats with companies that provide vital support to critical infrastructure, even if that data could be classified, and gave them 120 days to do so. Second, it directed government, led by the Director of Homeland Security, to create a flexible, risk-based framework of core practices for cyber, and allowed 240 days for a preliminary version of the framework to be presented to the President. Finally, the order put a high priority on the protection of privacy and civil liberties even as cybersecurity's strengthened.

The executive order certainly put the US ahead of Australia in setting clear policy approaches to critical infrastructure security from cyberattack. However, American structures and approaches are still evolving. They still face the same difficulties Australia does: the challenges of creating effective cross-departmental cooperation; a military–civilian and intelligence–law enforcement divide in cyber responsibilities; and a lack of financial capacity on the part of the policy leader tasked with herding the multiple cyber cats.

At the international level, the US has shown a determination to be more proactive and firm in setting out its cyber interests in international negotiations, which the State Department leads on, but in particular with China, which the US increasingly identifies as a principal cyber-aggressor. In a recent address, US National Security Advisor Thomas Donilon quite sharply outlined what he felt was required from a US perspective:

> Specifically with respect to the issue of cyber-enabled theft, we seek three things from the Chinese side … First, we need a recognition of the urgency and scope of this problem and the risk it poses—to international trade, to the reputation of Chinese industry and to our overall relations. Second, Beijing should take serious steps to investigate and put a stop to these activities. Finally, we need China to engage with us in a constructive direct dialogue to establish acceptable norms of behaviour in cyberspace.[15]

These efforts are clearly aimed at increasing the pressure on China to curb malicious activity in cyberspace and to address the matter through diplomatic negotiation. No longer will the cries of surprise, denials of involvement and claims of being the major victim of cyberattacks, rather than the instigator, be sufficient response to the multiple accusations against China. This message was reinforced in President Obama's first phone conversation to new Chinese President Xi Jinping. Obama addressed the issue of cyberattacks and his expectation that nations would adhere to international norms and rules. The Chinese responded that they were open to direct dialogue with the US on such issues.

The UK experience

The UK published its first cybersecurity strategy in 2009, which also led to the formation of two main departments to manage the issue:

- The Cyber Security Operations Centre is hosted at the UK's Government Communications Headquarters (GCHQ).
- The Office of Cyber Security and Information Assurance is based in the Cabinet Office, and provides the strategic leadership and coordination function for policy.

Other departments have a role within cybersecurity for the UK, including the Ministry of Defence, Department for Business, Innovation and Skills, the Home Office and other intelligence agencies. The international aspects of cybersecurity are led by the Foreign and Commonwealth Office, who have some 15 staff dedicated to this issue along with substantial funding.

The 2010 Strategic Defence and Security Review allocated £650 million over four years to establish the new National Cyber Security Programme to strengthen the UK's cyber capacity. The initial 2009 cyber policy was updated in 2011, and the UK national security strategy ranks cybersecurity as one of the top-tier risks to the nation's security.

One of the most forward-thinking ideas in the 2011 policy is the formation of the Cyber-Security Information Sharing Partnership between government and the private sector, which has grown from a pilot project run in 2011–12. Around 160 companies in the defence, finance, pharmaceuticals, energy and telecommunications sectors are able to share information on current threats and incident management practices via an online portal. Around 10 officers drawn from MI5, MI6 and GCHQ, as well as private sector secondees, coordinate the partnership's 'fusion' centre.

The UK has had problems in developing its framework due to interdepartmental frictions. The Centre for Protection of Critical National Infrastructure, traditionally responsible for this area, became reluctant to share responsibilities for cybersecurity with others. The UK has also recently established a Computer Emergency Response Team (CERT) for UK Government, borrowing the idea from its allies. By no means is the UK's approach perfect, but it shows far more coherence than it did five years ago.

British policy doesn't advocate the creation of a 'cyber czar', but it's known that Prime Minister Cameron takes a personal interest in the issue, which helps to drive the issues forward.

What should Australia do?

The Australian approach to cyber issues is maturing, but still requires further development so that the risk is truly understood by all sectors and appropriate responses are put in place.

Progress is evident in the fact that the 2013 National Security Strategy lists cyber as one of its key security concerns. The *Defence White Paper 2013* also marks a new stage in how cyber issues are dealt with by the Australian Government.

Emphasising a whole-of-government approach by renaming DSD to the Australian Signals Directorate is a welcome but limited step, but more substance must be added to the practical policy and administrative changes hinted at in such a move. More work is needed to ensure effective cooperation between departments, create productive mechanisms for the private sector to play its part, and provide enough money to produce results.

The absence of the Cyber White Paper reflects a major gap in Australia's national security policy. This must be addressed as a matter of urgency. In a rapidly technologically evolving environment, it's unacceptable for cyber policy to be left without updating for four years.

Because the update to the national digital economy strategy failed to cover the necessary cybersecurity territory, a Cyber White Paper must be re-commissioned and delivered in no more than 12 months. It should contain a clear examination of the threat picture in cyberspace to help government and business respond appropriately to changed or increased security requirements.

Issues to be covered in a Cyber White Paper

ASPI recommends seven essential components of a future Cyber White Paper.

1. Quickly strengthen cyber risk awareness, risk reduction measures and data sharing on threats to critical national infrastructure

The critical national infrastructure of a nation is its life-support system—the essential services and functions that keep it operating. It's increasingly clear that infrastructure is targeted for malicious purposes in cyberspace. Our response not only requires a whole-of-government approach, but must also incorporate critical infrastructure operators in all sectors. Most of them are in the private sector.

We currently have underfunded, inadequate mechanisms for raising risk awareness, reducing risk and sharing threat data. CERT Australia has been a good way for government to share some data with some critical infrastructure operators, but this needs to be expanded to include operators of infrastructure who perhaps aren't even aware that they're targeted. The government's already indicated that 'industry and other private sector partners' will be involved in the development of the ACSC.[16] But, again, the focus there will be on operational matters rather than higher level information-sharing to support a common policy response. Additionally for the private sector to become a key partner they need to be able to understand that there is a distinct 'product' for them to access and contribute to, and they need to be willing to share data with government, otherwise momentum will be lost and they won't keep their focus on such efforts.

Canberra should look closely at the model set out in Obama's executive order on improving critical infrastructure cybersecurity, which stipulated a stringent timeframe (120 days) for reforming information-sharing between government and the private sector and improving the volume, timeliness and quality of threat reporting. The order also set a one-year deadline for establishing a 'Cyber Security Framework', the purpose of which is to ensure that policy, business and technology are aligned to address cyber risks. It also proposed a consultative process with the private sector at the policy level, rather than just on technical responses to cyber risk.

Obama's timeframes are ambitious, but they bring home the sense of urgency and priority that his administration is giving to the task. The deadlines also contrast with the two years that have elapsed since the Australian Government's June 2011 announcement of a Cyber White Paper. After the 2013 election, the government should fast-track an effort to lift public awareness and response on cyber threats to critical infrastructure. The new government should aim for the delivery of an initial Cyber Security Framework document within 12 months.

2. Strengthen national cyber policymaking capabilities

Australia's current cyber policymaking capabilities require upgrading. The most effective cyber policies will address the whole-of-government dimension of the problem, incorporate private sector concerns and address public concerns about privacy and civil liberties. Against this test, Australia's cyber policy looks disjointed and lacking in detail. Better policy will derive from strong top-down leadership and coordination on the issue. The watchwords are 'leadership' and 'coordination'—cyber encompasses too many complex issues to be run as a single organisational function. Various aspects of implementation and 'tactical' policymaking must be devolved to those areas of government or industry best placed to deal with issues as they arise.

We need to develop a whole-of-government cyber *policy* capability that mirrors the *operational* focus of the ACSC. ASPI's not proscriptive about where such a capability should be administratively located, but PM&C or AGD are the two obvious areas.

It would be best if the new AGD-chaired whole-of-government committee created to oversee the ACSC is given the necessary resources and tasked to create a Cyber Policy Unit, drawing on skills from a wide range of interested parties. In time, the unit will develop to be the key to shaping government decision-making on cyber policy. A significant part of the Cyber Policy Unit's workforce will probably need to be 'virtual'—meaning that the unit must draw on skilled people in different agencies. Regardless of whether people move to a single location or collaborate virtually, what's critical is that the unit has the capacity to drive policy development to a rational conclusion and not simply act as a broker of compromises between agencies. Both PM&C and AGD will need to review the existing structures and positions they allocate to cyber. Perhaps PM&C's Cyber Policy Coordinator should head the Cyber Policy Unit.

This paper doesn't address ministerial arrangements for cyber, but it's clear that the diffusion of policy responsibility for cyber in the Budget reduces the government's capacity to respond effectively to cyber issues.

For example, an ABC TV *Four Corners* report on cyberespionage broadcast on 27 May 2013 alleged that the 'floor plans' for the new Canberra headquarters of the Australian Security Intelligence Organisation had been stolen in an espionage operation: 'someone had mounted a cyber hit on a contractor involved in the site. The plans were traced to a server in China.'[17] The government responded to this issue through comments offered by the Attorney-General as part of the program and later by the Foreign Minister and the Prime Minister in parliament. This diffuse ministerial responsibility for cyber issues creates risk for government that can be addressed by developing clearer lines of reporting to ministers and the Cabinet.[18]

3. Build more effective relations with the private sector to harness its skills and capacities and to strengthen resilience

Government needs to develop clearer mechanisms to collaborate with the private sector on cyber issues, as well as ensuring that the government have a viable 'product' with which the private sector can engage. There's consultation on operational matters through CERT Australia, and it's also promised for the ACSC, but the absence of a consultative process at a higher decision-making level became distressingly obvious in the non-appearance of the Cyber White Paper. A review of the PM&C and DBCDE websites shows that they give little guidance about the white paper process, but much information that's patently out of date.[19]

While many policy documents, including the recent Defence White Paper, acknowledge that a clearer relationship with the private sector needs to be defined, the rules of engagement are not stated. Mechanisms for discussion and practical work need to be developed as a matter of urgency so that the private sector can be part of the cyber solution. After the 2013 election, the new government should direct the AGD secretary-level committee reporting to Cabinet on cyber to establish a Business Advisory Network on Cyber Security. The network would advise the committee on private sector perspectives at the senior board level.

A new Cabinet would benefit from a regular opportunity to meet senior business leaders to discuss the shared challenge of cybersecurity. The Prime Minister's Science, Engineering and Innovation Council—the pre-eminent science advisory body to government—would be an effective model. Chaired by the Prime Minister and with a membership comprising ministers, the Chief Scientist and a select group of experts, the council meets three times a year to advise government on scientific and technological developments.[20] The government should establish a Prime Minister's Cyber Council along the same lines to bring government and the private sector together at the CEO–ministerial level to consider cybersecurity policy. Such a group would certainly meet the Business Council of Australia's call to 'identify … where government and industry can work together to enhance security for businesses at risk of cyber-attack'.[21]

4. Consolidate community advice on cyber issues

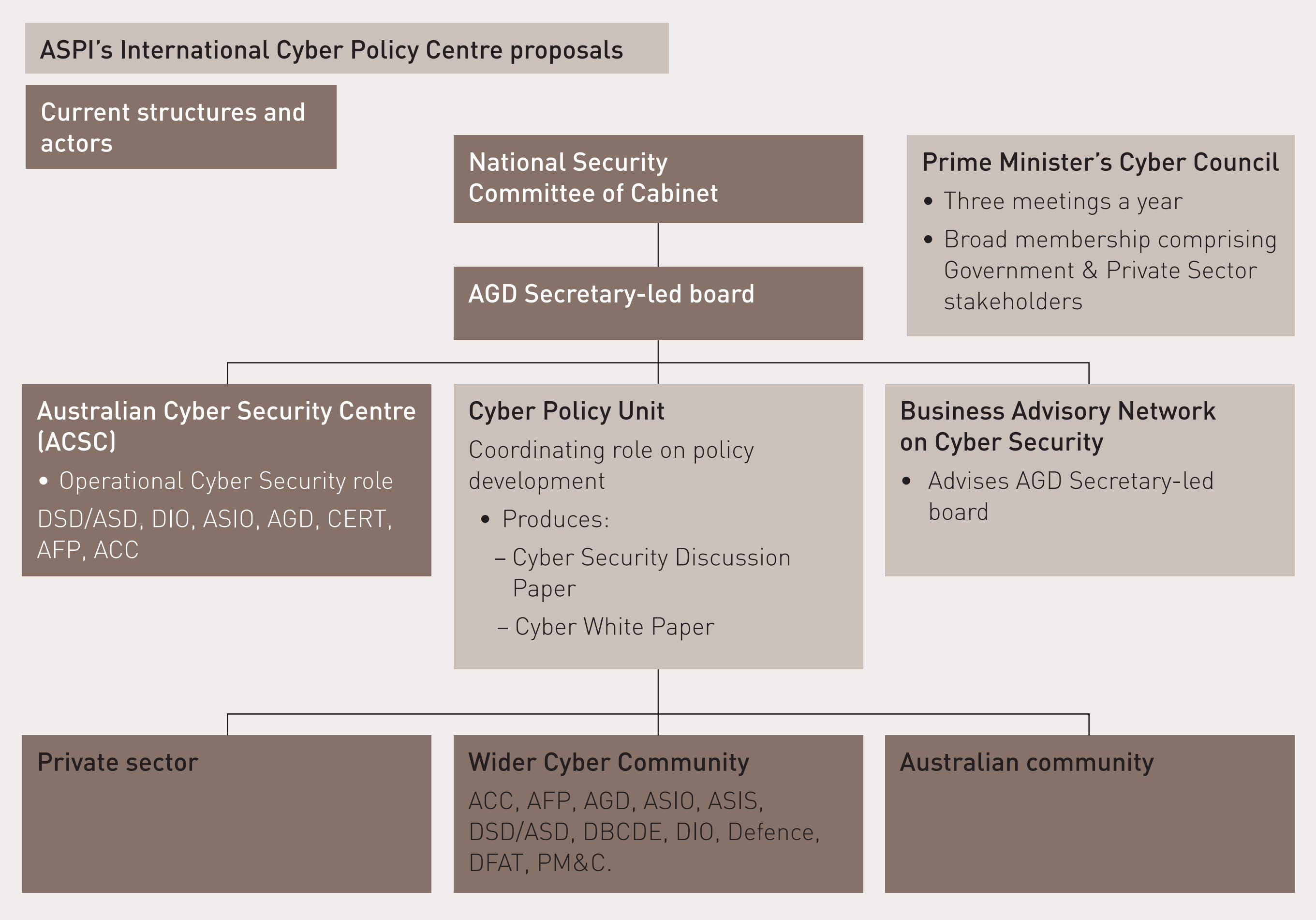
A plethora of government agencies currently offer outreach programs to the community on different aspects of cybersecurity. They include the TISN run by AGD, made up of seven sector groups, two expert advisory groups, communities of interest and the Critical Infrastructure Advisory Council. A visitor to the DBCDE's website is quickly adrift in a sea of acronyms: 'CIAC, as the peak body of TISN, oversees the IAAGs along with the EAGs and provides advice to the Attorney-General on the National Approach to CIR.'[22]

The DBCDE website directs people concerned about personal internet security to an astonishing array of initiatives. There's a National Cyber Security Awareness Week; a Cyber Security website; a Stay Smart Online Alert Service; Budd:e cybersecurity and safety education modules; an internet service providers' voluntary code of practice; an Australian Internet Security Initiative run by the Australian Communications and Media Authority; and yet further programs on fraud awareness, content regulation, spam and online gambling.[23] DSD, perhaps one of the government's lowest-profile agencies, has its own extensive range of cyber outreach programs, ranging from very detailed and practical advice on Strategies to Mitigate Targeted Cyber Intrusions[24] through to its Catch, Patch, Match awareness campaign, with a stylistic resemblance to Pink Panther cartoons.[25]

This only begins the list of cybersecurity-related material generated by government agencies and available to the public. Clearly messages need to be tailored to their audience, what a parent needs to know about online safety for their child would differ to what a multinational company needs to know in order to protect itself from large-scale data theft. However, there is currently a real challenge for users of government information to know which of it, if any, might meet their needs.

The government should audit its cyber-related public information campaigns and streamline the number of offerings. The AGD secretaries' committee should become an approval authority for any such campaign. The Cyber White Paper should present a structured program of information campaigns designed to target specific sectors, such as small and medium-sized

Table 2: ASPI – ICPC proposed enhancements to cybersecurity policy mechanisms



ASPI's International Cyber Policy Centre proposals

Current structures and actors

National Security Committee of Cabinet

AGD Secretary-led board

Prime Minister's Cyber Council

- Three meetings a year
- Broad membership comprising Government & Private Sector stakeholders

Australian Cyber Security Centre (ACSC)

- Operational Cyber Security role

DSD/ASD, DIO, ASIO, AGD, CERT, AFP, ACC

Cyber Policy Unit

Coordinating role on policy development

- Produces:
  - Cyber Security Discussion Paper
  - Cyber White Paper

Business Advisory Network on Cyber Security

- Advises AGD Secretary-led board

Private sector

Wider Cyber Community

ACC, AFP, AGD, ASIO, ASIS, DSD/ASD, DBCDE, DIO, Defence, DFAT, PM&C.

Australian community

enterprises, schools, individual IT users and groups with specific needs. As in all government advertising, the challenge is to control the volume of material offered and to ensure that it's of a uniform quality, with consistent messaging.

5. Determine how to strengthen cyber cooperation with the US

Although there are differences of opinion at times with the US, Australian defence and intelligence cooperation with the US on cyber has the potential to become part of the core of our practical strategic relationship. An important step forward was taken at the September 2011 Australia–US Ministerial Consultation meeting, when a joint statement on cyber was issued. In effect, the statement applied the terms of the ANZUS Treaty to a cyberattack:

> … in the event of a cyber attack that threatens the territorial integrity, political independence or security of either of our nations, Australia and the United States would consult together and determine appropriate options to address the threat.

The statement also committed the two countries to collaborate in the international community 'to advance the development of international norms for cyberspace'.[26]

While cyber cooperation with the US is close in the traditional spheres of defence and intelligence engagement, more work needs to be done to align policy approaches to domestic security and international diplomacy.

On domestic cybersecurity issues, Australia and the US would benefit from aligning our policy approaches as closely as possible. The business sector in both countries needs some assurance that approaches that work in one jurisdiction will meet standards and requirements in the other. This isn't a trivial matter, given that the US is the largest provider of foreign direct investment in Australia and that the combined foreign direct investment of each country in the other is valued at over a trillion dollars.[27] American firms investing in Australia will look for assurance that their cyber interests are well protected and that our national policies are as coherent as Obama's executive order intends for the US. Australia and the US should aim to achieve a single standard for cybersecurity.

In international diplomacy, the requirement is for Australia and the US to deepen our understanding about what the international community should do to strengthen a free and secure 'cybercommons'. Cyber is emerging as a discussion point in all US bilateral dialogues. In May 2013, the US held its first cyber dialogue with Japan[28] and foreshadowed discussions with China on the same topic. Australia needs to understand America's intent here. Until only recently, cyber information tended to be very closely held and the subject of discussions only between close allies. While those classified conversations will continue, it's clear that cyber is so ubiquitous in business, personal and international life that it's forced itself onto the bilateral and multilateral agendas of countries around the world. While Canberra and Washington will pursue their interests separately as well as together in multilateral meetings, we should make sure that our approaches complement each other's and advance our shared interests.

The Cyber White Paper should set out a strategy to achieve that objective. This inevitably will require closer dialogue with Washington in a way that involves peak business bodies and law enforcement and internal security agencies.

6. Develop a strategy on how to engage China on cyber

Australia's strategically aligned with the US but enjoys a very close economic and trade relationship with China. This brings both risks and opportunities, especially in relation to cybersecurity. Clearly, the US expects Australia to play a lead role in the Asia–Pacific region in promoting an open and safe online environment that allows economic growth alongside freedom of expression. While we're well placed to help in building regional capacity to understand cyber risks and responses, and in building sensible cyber policy, this approach might potentially create tension with China, which is often seen as a main instigator of the malicious use of cyberspace.

China's role as a potentially malign actor in cyberspace has become too high-profile to be ignored. In response to *Four Corners*' allegations about Chinese espionage to obtain floor plans of the new Australian Security Intelligence Organisation building, the Australian Foreign Minister simply dismissed the issue, saying 'There are no implications for our strategic partnership … When it comes to China every Australian knows how economically important it is to this country to have the relationship with China that we have today.'[29]

That's not a sustainable position. Australia needs to engage China in a dialogue about cyber issues so that some common ground and limitations on cyber activities can be set out, especially as economic growth in our region is going to make the matter even more important. During her April 2013 visit to China, former Prime Minister Gillard indicated that she raised cybersecurity in her discussions with Premier Li Keqiang.[30] Canvassing the issue will need to become a substantive feature of Australian engagement with China in coming years.

7. Develop a regional engagement strategy

Just as we should deepen our cyber conversation with the US and China, we need to do so with other key international players and with our wider region. In October Australia will have a major diplomatic opportunity to show some intellectual creativity on cyber matters at the third international Conference on Cyberspace in Seoul. It's expected that 800 government, business and NGO delegates from more than 80 countries will attend. They'll discuss their 'vision for cyberspace' and ways to strengthen cross-border cooperation, boost economic growth and development, fight cybercrime and build international cybersecurity.[31]

The Seoul conference will be an early and demanding challenge for the new Australian Government. It will need to quickly brief Australian delegates and set out a plan that articulates a coherent approach to the main issues under debate, including how to develop appropriate international norms of behaviour in cyberspace, how to respond to Russian and Chinese proposals for greater international regulation of the internet, and how to collectively address malign cyber behaviour.

The timing of the conference means that Australia can use it to inform the development of the Cyber White Paper, and particularly the strategy that we should adopt for discussing cyber issues with our friends and neighbours. It is strongly recommended that the Australian Foreign Minister attend the conference to match the same level of representation of our close allies, and demonstrate the nation's commitment to creating rules of the road on the malicious use of cyberspace. In Southeast Asia, the ASEAN Regional Forum provides a vehicle from which Australia can start a dialogue on cybersecurity. There is a wide spectrum of cyber capabilities in the region, from almost non-existent to remarkably sophisticated. In the broad, Australia's strategic interest would be helped if Asia–Pacific countries were able to develop some aligned approaches to cybersecurity. International discussions around articulating shared norms of behaviour in cyberspace are a starting point to that broader objective. As Australia's regional engagement strategy for cyber develops, the need will be to determine how best to contribute to the dialogue on norm formation, the creation of regional confidence-building measures, and how to help strengthen the cyber resilience of key regional friends.

If Australia is to take on a higher profile role in regard to international cyber issues it follows that DFAT would need to increase the level of resource and focus that it places upon these issues, as they would logically be the lead department for international diplomatic engagement.

Two steps to help deliver a Cyber White Paper

The seven areas identified above for inclusion in a Cyber White Paper are obvious and important steps that government must take quickly to set out a more orderly approach to a rapidly growing national priority. As President Obama's approach has shown, there's value in pushing for a quick outcome by setting a 12-month deadline. A sense of high priority should cut through some of the Canberra turf wars that have slowed policy work. While the Australian Public Service and other agencies haven't deliberately set out to delay the work, they've struggled to deal with a novel set of policy issues that don't easily fit into traditional bureaucratic structures. Some senior-level political push is needed to break the inertia.

Two interim steps will help ease the way for the drafters of the Cyber White Paper. First, the government should quickly establish the proposed Prime Minister's Cyber Council and appoint senior CEOs, officials and cyber experts as its members. The council should be given the task of shaping a broad public debate about the challenges, opportunities, risks and rewards of cybersecurity. Governments will know that their cyber policies will be well received when the standard of public debate about cyber matters approaches the sophistication we see in the Australian media on economic policy. We're some way from that point, but an empowered and active Cyber Council could help enormously.

Second, the Prime Minister's Cyber Council (working with the AGD-led whole-of-government secretaries' committee) should develop a public discussion paper on cybersecurity, similar to defence policy discussion papers issued before the 2000 and 2009 Defence white papers. The paper shouldn't reflect settled policy, but set out a balanced discussion on some critical issues such as how to treat privacy concerns, how to balance government and private sector responsibilities, the value of measures to regulate the internet, and how to shape an international consensus on cybersecurity. It should be issued around the six-month point of the 12-month white paper process.

ASPI's International Cyber Policy Centre

ASPI's come to the view that there's a pressing need to be involved in the emerging policy debates on cybersecurity. There are two such debates: one at an often very highly classified government level, and one that encompasses a wider group in civil society but is often limited to those with deep specialist knowledge about information technology and security. There's a need for a broader dialogue among people interested in many aspects of the impact of cyber issues on public policymaking.

With this in mind, ASPI is establishing an International Cyber Policy Centre that has four key aims:

- Lift the level of Australian and Asia–Pacific public understanding and debate on cybersecurity.
- Provide a focus for developing innovative and high-quality public policy on cyber issues.
- Provide a means to hold Track 1.5 and Track 2 dialogue on cyber issues in the Asia–Pacific region.
- Link different levels of government, business and the public in a sustained dialogue on cybersecurity.

These efforts will be at the national and international levels and look to enhance the cybersecurity of Australia and the region. There's currently no centre in Australia or Asia that provides a focused research and strategic outreach program on the national and international development of the 'rules of the road' and confidence building measures for the cyberdomain.

One of the ASPI International Cyber Policy Centre's core principles will be to ensure that both private sector and public sector voices are heard and considered. The internet is mainly in the hands of the private sector and civil society, so their opinions are essential if we're to build lasting cyber norms that don't constrain innovation and commerce, and that make cyberspace a secure place.

Conclusion

This paper sets out an approach that would help the Australian Government to rapidly develop a Cyber White Paper. While Australia's operational management of cybersecurity risk has been competent at the technical level, we've failed to grasp the nettle in developing sensible policy approaches.

A rapid policy development effort over 12 months, building on work already done, has the potential to jolt the system into more effective action. Failure to take this path would put Australia at risk of falling behind rapid cybersecurity developments in the US and other key friends and allies.

The need now is for quick-thinking political leadership to sustain Australia's strong advantages in cyber and to build a cyber leadership position for us in the international community.

Notes

[1] Department of the Prime Minister and Cabinet (PM&C), *Strong and secure: a strategy for Australia's national security*, January 2013, available from http://www.dpmc.gov.au/national_security/national-security-strategy.cfm); Department of Defence (DoD), *Australian cyber security centre to be established*, 24 January 2013, available from http://www.defence.gov.au/defencenews/stories/2013/jan/0124.htm.

[2] White House, *Executive Order—Improving critical infrastructure cybersecurity*, 12 February 2013, available from http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity.

[3] See David E Sanger, 'In cyberspace, new Cold War', *New York Times*, 24 February 2013, available from http://www.nytimes.com/2013/02/25/world/asia/us-confronts-cyber-cold-war-with-china.html?pagewanted=all&_r=0); Mandiant Corporation, *Exposing one of China's cyber espionage units*, Mandiant Intelligence Centre report APT1, available from http://intelreport.mandiant.com/).

[4] Australian Government, *Cyber Security Strategy*, 2009, available from http://www.ag.gov.au/RightsAndProtections/CyberSecurity/Documents/AG%20Cyber%20Security%20Strategy%20-%20for%20website.pdf .

[5] Prime Minister and Minister for Defence, '2013 Defence White Paper: renaming the Defence Signals Directorate and the Defence Imagery And Geospatial Organisation', media release, 3 May 2013, available from http://www.pm.gov.au/press-office/2013-defence-white-paper-renaming-defence-signals-directorate-and-defence-imagery-and-g.

[6] PM&C, 'Statement by the Secretary—3 June 2011 announcement of the Cyber White Paper', media release, 3 June 2011, available from http://www.dpmc.gov.au/media/statement_2011_06_02.cfm.

7 See http://www.ag.gov.au/RightsAndProtections/CyberSecurity/Pages/default.aspx.

8 Julian Bajkowski, 'Conroy seizes cyber whitepaper', GovernmentNews.com.au, 29 October 2012, available from http://www.governmentnews.com.au/2012/10/29/article/Conroy-seizes-Cyber-whitepaper/QMDSHZDJFA.html; Paul Maley, 'Downgrade for cyber white paper', *The Australian*, 29 January 2013, available from http://www.theaustralian.com.au/national-affairs/defence/downgrade-for-cyber-security-white-paper/story-e6frg8yo-1226563800851; Prime Minister, Closing remarks to the Digital Economy Forum, 5 October 2012, available from http://www.pm.gov.au/press-office/closing-remarks-digital-economy-forum.

9 DBCDE, *Advancing Australia as a Digital Economy: An update to the National Digital Economy Strategy* 12 June 2013. Available at http://www.nbn.gov.au/files/advancing_australia/index.html.

10 The roles of the Deputy National Security Adviser are detailed at http://www.dpmc.gov.au/national_security/index.cfm.

11 DoD, *Defence White Paper 2013*, para. 2.90, p. 21, available from http://www.defence.gov.au/whitepaper2013/docs/WP_2013_web.pdf.

12 Business Council of Australia, *Submission to the Department of the Prime Minister and Cabinet regarding the Digital Economy White Paper*, January 2013, available from http://bca.com.au/Content/102083.aspx.

13 Richard A Clarke and Robert K Knake, *Cyber war: the next threat to national security and what to do about it*, Harper Collins, New York, 2010.

14 Ryan Singel, *White House cyber czar: 'There is no cyberwar'*, Wired, 4 March 2010, available from http://www.wired.com/threatlevel/2010/03/schmidt-cyberwar/.

15 Thomas Donilon, quoted in Zachary Fryer-Biggs, 'Donilon: White-House "will take action" against cyber threats from China, *Defense News*, 11 March 2013, available from www.defensenews.com/article/20130311/DEFREG02/303110016/Donilon-White-House-8216-Will-Take-Action-8217-Against-Cyber-Threats-from-China?odyssey=tab|topnews|text|FRONTPAGE.

16 DoD, *Defence White Paper 2013*, para. 2.91.

17 Andrew Colvin and Peter Cronau, 'Hacked!', *Four Corners*, ABC TV, first broadcast 28 May 2013, transcript available from http://www.abc.net.au/4corners/stories/2013/05/27/3766576.htm#transcript.

18 Adam Gartrell, 'Spy claim no threat to China ties, Carr', *Herald Sun*, 28 May 2013, available from http://www.heraldsun.com.au/news/breaking-news/carr-refuses-to-confirm-china-hack-claims/story-fni0xqi4-1226651879092.

19 For example, PM&C has not updated references to the 'broadening' of the Digital Economy White Paper and still announces that a Cyber White Paper is being developed (http://www.dpmc.gov.au/media/statement_2011_06_02.cfm). DBDCE's website staysmartonline.gov.au still carries references to the Cyber White Paper (http://www.staysmartonline.gov.au/cyber_white_paper), but the links to further information are now inactive. A search on the words 'White paper' on DBCDE home page does not bring up any reference to the Digital Economy White Paper.

20 For details on the council, see: http://www.innovation.gov.au/science/pmseic/Pages/default.aspx.

21 Business Council of Australia, *Submission to the Digital Economy White Paper*.

22 DBCDE, *Communications critical infrastructure resilience*, 27 May 2011, available from http://www.dbcde.gov.au/online_safety_and_security/Communications_critical_infrastructure_resilience.

23 These activities and programs are set out on the DBCDE website at http://www.dbcde.gov.au/online_safety_and_security.

24 Available from http://www.dsd.gov.au/infosec/top35mitigationstrategies.htm.

25 Available from http://www.dsd.gov.au/videos/catch-patch-match.htm.

26 Kevin Rudd, *Joint Statement on Cyberspace*, 15 September 2011, available from http://foreignminister.gov.au/releases/2011/kr_mr_110916a.html.

27 Kim Beazley, 'Cheap energy revives the US for Aussie business investors', *The Australian*, 16 May 2013, available from http://www.theaustralian.com.au/national-affairs/opinion/cheap-energy-revives-the-us-for-aussie-business-investors/story-e6frgd0x-1226643393364).

[28] US Department of State, *Joint Statement on US–Japan Cyber Dialogue*, 10 May 2013, available from http://www.state.gov/r/pa/prs/ps/2013/05/209238.htm.

[29] Lanai Scarr, 'Bob Carr says relationship with China remains strong despite cyber attack on ASIO', *News.com.au*, 28 May 2013, available from http://www.news.com.au/national-news/federal-election/bob-carr-says-relationship-with-china-remains-strong-despite-cyber-attack-on-asio/story-fnho52ip-1226651933695).

[30] Prime Minister Gillard, *Transcript of joint press conference, Beijing*, 9 April 2013, available from http://www.pm.gov.au/press-office/transcript-joint-press-conference-43.

[31] The conference program is available from http://www.seoulcyber2013.kr/index.html.

Acronyms and abbreviations

ACSC	Australian Cyber Security Centre
AGD	Attorney-General's Department
CERT	Computer Emergency Response Team
DBCDE	Department of Broadband, Communications and the Digital Economy
DSD	Defence Signals Directorate
GCHQ	Government Communications Headquarters (UK)
NGO	non-government organisation
NSCIO	National Security Chief Information Officer
PM&C	Department of the Prime Minister and Cabinet
TISN	trusted information sharing network

About the authors

Peter Jennings is the Executive Director at ASPI.

Tobias Feakin is ASPI's senior analyst specialising in national security.

Important disclaimer

This publication is designed to provide accurate and authoritative information in relation to the subject matter covered. It is provided with the understanding that the publisher is not engaged in rendering any form of professional or other advice or services. No person should rely on the contents of this publication without first obtaining advice from a qualified professional person.

About Special Reports

Generally written by ASPI experts, Special Reports are intended to deepen understanding on critical questions facing key strategic decision-makers and, where appropriate, provide policy recommendations. In some instances, material of a more technical nature may appear in this series, where it adds to the understanding of the issue at hand. Special Reports reflect the personal views of the author(s), and do not in any way express or reflect the views of the Australian Government or represent the formal position of ASPI on any particular issue.

ASPI
Tel +61 2 6270 5100
Fax + 61 2 6273 9566
Email enquiries@aspi.org.au
Web www.aspi.org.au

RRP $5.00 ISSN 2200-6648

BECOME A MEMBER

JOIN NOW TO RECEIVE PRINTED PUBLICATIONS AND MORE

Join Australia's liveliest minds writing today on defence and strategic issues. ASPI produces ***Strategy***, ***Strategic Insights***, ***Special Reports***, and specialist publications including ***The Cost of Defence*** and an upcoming ADF capability annual.

ASPI's work is at the cutting edge of new thinking on defence and security.

Thoughtful, ground-breaking and often controversial, ASPI leads the public debate on these issues. Become a valued part of the ASPI team today!

Join now and we will post your choice of 3 free publications from our recent publications list.

Future subjects include:

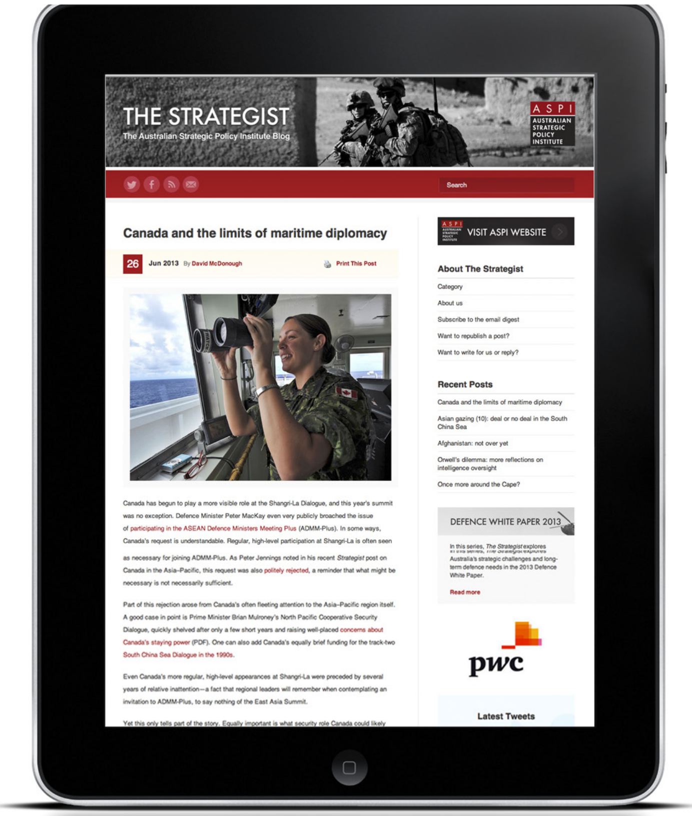
- **Australia as a Southern Hemisphere power**
- **Australia's defence cooperation program**
- **Implications for strategic changes in the Middle East**
- **Options for Australia–Indonesia cooperation**
- **Maritime rivalries in the Indo-Pacific**
- **ADF capability annual**

ASPI AUSTRALIAN STRATEGIC POLICY INSTITUTE
The Cost of Defence
ASPI Defence Budget Brief 2013–2014
Sixty-nine mi
eighty-one th
& eighty doll
per day
STRATEGY
ASPI
Planning the unthinkable war
'AirSea Battle' and its implications for Australia
Benjamin Schreer
April 2013
STRATEGY
ASPI
Facing the dragon
China policy in a new era
May 2013
ASPI AUSTRALIAN STRATEGIC POLICY INSTITUTE

Stay informed via the field's leading think tank, the Australian Strategic Policy Institute.

BLOG

ASPI's blog, **The Strategist**, delivers fresh ideas on Australia's defence and strategic policy choices as well as encouraging discussion and debate among interested stakeholders in the online strategy community. Visit and subscribe to an email digest at www.aspistrategist.org.au. You can follow on Twitter (@ASPI_org) and like us on Facebook (www.facebook.com/ASPI.org).



THE STRATEGIST
The Australian Strategic Policy Institute Blog

A S P I
AUSTRALIAN STRATEGIC POLICY INSTITUTE

Search

Canada and the limits of maritime diplomacy

26 Jun 2013 By David McDonough

Print This Post

Canada has begun to play a more visible role at the Shangri-La Dialogue, and this year's summit was no exception. Defence Minister Peter MacKay even very publicly broached the issue of participating in the ASEAN Defence Ministers Meeting Plus (ADMM-Plus). In some ways, Canada's request is understandable. Regular, high-level participation at Shangri-La is often seen as necessary for joining ADMM-Plus. As Peter Jennings noted in his recent *Strategist* post on Canada in the Asia–Pacific, this request was also politely rejected, a reminder that what might be necessary is not necessarily sufficient.

Part of this rejection arose from Canada's often fleeting attention to the Asia–Pacific region itself. A good case in point is Prime Minister Brian Mulroney's North Pacific Cooperative Security Dialogue, quickly shelved after only a few short years and raising well-placed concerns about Canada's staying power (PDF). One can also add Canada's equally brief funding for the track-two South China Sea Dialogue in the 1990s.

Even Canada's more regular, high-level appearances at Shangri-La were preceded by several years of relative inattention—a fact that regional leaders will remember when contemplating an invitation to ADMM-Plus, to say nothing of the East Asia Summit.

Yet this only tells part of the story. Equally important is what security role Canada could likely

VISIT ASPI WEBSITE

About The Strategist

- Category
- About us
- Subscribe to the email digest
- Want to republish a post?
- Want to write for us or reply?

Recent Posts

- Canada and the limits of maritime diplomacy
- Asian gazing (10): deal or no deal in the South China Sea
- Afghanistan: not over yet
- Orwell's dilemma: more reflections on intelligence oversight
- Once more around the Cape?

DEFENCE WHITE PAPER 2013

In this series, *The Strategist* explores Australia's strategic challenges and long-term defence needs in the 2013 Defence White Paper.

Read more

pwc

Latest Tweets

A S P I
AUSTRALIAN
STRATEGIC
POLICY
INSTITUTE

To find out more about ASPI and membership go to www.aspi.org.au
or contact us on 02 6270 5100 and enquiries@aspi.org.au.