# Submission to the National Commission of Audit from the Australian Strategic Policy Institute
## Submission Two: National Security

This submission addresses the National Commission of Audit's terms of reference in the area of national security, with particular reference to policing and cybersecurity.

Australians' ideas about national security have changed as the nation has become wealthier and more technologically advanced over the past two decades or so. Today, security is no longer exclusively about existential threats, such as war, but also about terrorism, crime and threats generated through the internet. This change introduces three new dynamics into Australia's political debates.

The first dynamic is the broadening of security activities. Australia's Cold War concerns about nuclear war and decolonisation in Asia receded as the Soviet Union collapsed, the international community recognised China, and Southeast Asian states became more internally coherent. However, those same changes allowed different state and non-state actors to pursue their interests with fewer constraints, leading to a number of internal wars and another round of international atomisation. As a consequence, Australia launched or participated in various overseas operations designed to achieve political, economic and humanitarian objectives, and used a broad mix of national capabilities to do so—diplomats, police, aid workers and the Australian Defence Force.

The second dynamic is the greater range of vulnerabilities we face today. Wealth, connectivity and convenience have increased the potential for economic and social disruptions, and also Australians' expectations of their governments. Increasingly, managing the vulnerabilities of critical industrial, commercial and transport infrastructure is becoming beyond the capacity of its operators. Our weak points could be tested by maleficent actors for political or economic gain, or by natural disasters, and this makes government's role essential. But, as the public's expectations increase, demarcating the government's responsibility becomes a difficult political question.

The third dynamic is the way security concerns can touch ordinary citizens, every day. In the decades after World War II, even our military operations have required only a little sacrifice from most of us. Today, and into the immediate future, security threats such as organised crime, cybercrime and border security challenges can and will affect Australians' neighbourhoods and homes. Widespread diasporas, increasing connectivity and the power of traditional and new media make global problems more immediate and often more local. This makes security a mainstream concern and a regular—not exceptional—part of Australian political life. Australians are looking to government to protect their way of life, and sometimes to advance their ideals, to a more individual and more immediate level.

These three dynamics will continue to influence the priorities and draw on the resources of all Australian governments, and require closer cooperation among them and with our international partners.

## Australian priorities

In ASPI's view, the three new dynamics lead to three priorities for national security policymaking.

First, we need to get a better understanding of how the dynamics affect Australia's interests. This means understanding change across the globe, across the region and within Australia. It requires detailed consideration of how information flows and how technology, resources and money move. It also requires the ability to make cold-eyed calculations about whether an event or a change really affects Australia's security—and in some cases to explain why the latest problem should not consume our resources. At present, Australia's ability to perform this critical analysis is mature and generally very effective, although there's a bias towards understanding the interactions and intentions of nation-states over other important actors, especially sub-state groups that aren't directly involved in conflict.

Second, we need to create a 21st century response to 21st century challenges. Our Constitution and political system have proven robust so far, in that the system allows the Australian Government to act in the national interest, but can nevertheless constrain necessary action. For example:

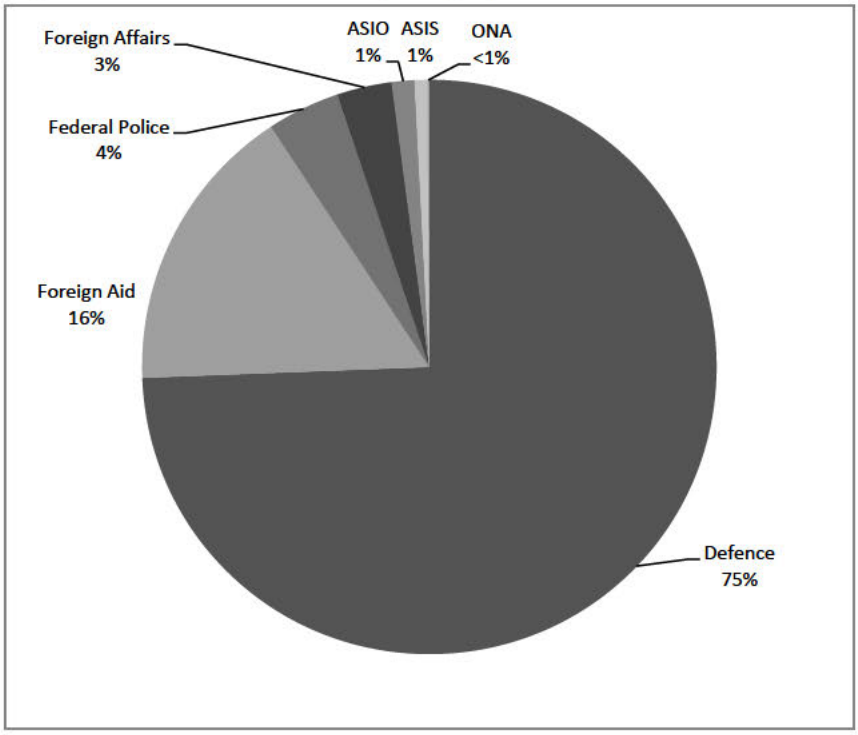
- State and federal cooperation on security issues is now more important than ever, but the mechanisms and funding for that cooperation have developed in an ad hoc way, issue by issue. This means we have a plethora of overlapping committees, ministers and officials, especially in the policy development space. It also means the Commonwealth has needed to fund efforts to build nationwide capability to manage security threats, but it has done so in an inconsistent way.
- Importantly, criminals are able to exploit gaps in legislation among jurisdictions. And even in areas where the Commonwealth clearly has sole responsibility, such as in the cyberdomain, coordination has been patchy at best. We need new thinking that builds national awareness, ensures that we have the capabilities to deal with threats when and where they arise, links the substantial criminal information holdings of Australian governments, and seeks sensible economies of effort.

Third, we need more effective and sophisticated ways to engage the business and community sectors in security efforts, especially against organised crime, cybercrime and violent extremism.

## Resourcing national security

The Australian Government's allocation of resources to meet national security risks is currently heavily skewed towards defence spending (Figure 1). This is understandable, given the long lead-times and increasing cost of defence capability, but the government's own January 2013 National Security Strategy shows that five of the seven major risks to our national security have substantial non-defence components. While we can't compare the risks objectively without knowing the likelihood and consequence of each, we can infer two points that are very important for resource allocation across the national security community.

**Figure 1: The national security budget, 2012–13**




Source: 2013–14 Cost of Defence, ASPI Defence Budget Brief.

First, national security risks with a mainly domestic focus receive only a small part of the Australian Government's money. It's likely that efforts to counter domestic terrorism and organised crime and to protect our critical infrastructure and cybersecurity account for only 3%–4% of Commonwealth spending. Of course, state governments bear a reasonable share of the burden, too, but any objective risk assessment is likely to find that these dimensions of security are not resourced adequately to reduce the actual level of risk.

Second, the government has not presented a clear explanation of the relative risk of each of the eight challenges listed in the National Security Strategy. This means that it's not possible to determine whether resource allocations are flowing from risk assessments or from historical spending patterns. Better information would lead to more rational arguments about resourcing priorities. The National Commission of Audit might wish to consider asking for such an assessment.

## Policing and law enforcement

Over the past century there has been a steady growth in the range of crimes that can be perpetrated against the community and the nation. Australia's state governments were able to deal with most major criminal activities at Federation, but the Commonwealth's role in law enforcement has become more important with technological developments, our increasing prosperity, and the growing irrelevance of domestic and international borders to criminal enterprises. This change has had major implications for all Australian governments and made close cooperation among them essential.

Changes in the extent, vectors and nature of crime have made the Commonwealth's powers more directly relevant to law enforcement at the state and local levels. For example, the

Commonwealth's responsibility for telecommunications is now critical to combating cyber-fraud and identify theft; its corporations powers are used to prosecute major economic crimes; and its responsibility to protect the states from domestic violence has been a rallying-point in the national fight against terrorism. Less noted has been national agencies' generation of criminal intelligence, which is shared among the jurisdictions, and their leadership in law enforcement partnership arrangements with our regional neighbours and other countries.

These trends are unlikely to be reversed and may accelerate in some areas.

Overseas, the increasing fragility of some states and their need to build the rule of law are likely to lead to Australian law enforcement contributions in addition to, or perhaps in place of, traditional military contributions.

Within Australia, the states may refer more powers to the Commonwealth as it becomes clear that legal innovations such as unexplained wealth laws are best pursued on a national basis. There's also a pressing need for the Commonwealth to lead the multijurisdictional effort against organised crime by encouraging consistent, nationwide policing capabilities.

One such area is in the production and distribution of criminal intelligence, where the national agencies already contribute heavily. The breadth of inputs to this intelligence is expanding with the inclusion of taxation, immigration, customs and social security information. This kind of aggregation will require careful management, especially in relation to privacy, but will provide an essential weapon for law enforcement officers. However, the resources devoted to this function, especially through the Australian Crime Commission, are decreasing. This is a false economy.

While the Commonwealth should not seek new power unjustifiably, it must be alert to where its mandate and resources can be best used to ensure a national approach to fighting crime.

## Cybersecurity

The 21st century is going to be defined by the cyberdomain. Cyberspace already enables much of our economy and infrastructure, allows us to develop our defence, security, intelligence and social capital, and has created intimate interdependencies between states and new avenues for governments and non-state actors to achieve their policy, financial, military, political, ideological or social objectives in the physical world. Like most technologies, cyberspace is agnostic to politics and ideology, but is a powerful transfer mechanism for both.

Cyberpower is attractive to state and non-state actors because of its low relative cost, high potential impact and general lack of transparency. They can combine cyberpower with existing military capabilities and economic assets. Less powerful actors can gain asymmetrically by inflicting extensive damage on vulnerable targets by bringing down networks or stealing valuable information.

Threats in cyberspace cross multiple national jurisdictions with increasing frequency, so cybersecurity is rapidly emerging as a high-priority policy challenge for the Australian Government. The National Security Strategy lists 'malicious cyber activity' as the third of

seven key national security risks and calls for closer partnerships with the business community to develop a more effective response.

One problem is the large 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 is really much larger and growing.[1] The *Intelligence Services Act 2001*, which governs the operations of the Australian Signals Directorate (ASD), gives the agency responsibility for information security across all government operations, not simply Defence. ASD'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, 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 then Prime Minister announced the creation of the Australian Cyber Security Centre (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.

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.

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 those matters rise among national priorities, 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.

The most recent organisational reshuffles in cyber policy were announced in May in the 2013 Defence White Paper with the renaming of the Defence Signals Directorate as 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.'[2]

In effect, we've returned to the situation that applied in 2009: The Attorney-General's Department 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 the Attorney-General's Department 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'.[3]

It follows that a new government must embark on an urgent remediation strategy to strengthen Australia's cyber policy and crisis management structures. In July 2013, Peter Jennings and Tobias Feakin set out an ASPI agenda for cyber policy reform in *The emerging agenda for cybersecurity* (copy attached). The essence of our recommendations is as follows:

- Develop a Cybersecurity White Paper within 12 months of the election.
- To promote community and business engagement in the White Paper process, commission a cybersecurity discussion paper to be released within six months of the election.
- Strengthen contact with the business community at senior levels to build a broad public–private partnership on cybersecurity.
- Establish a Prime Minister's Cyber Council, comprising leading business CEOs, senior officials and cyber specialists to meet two or three times a year to discuss cybersecurity threats, challenges and solutions.
- Establish a cyber policy unit, reporting to the Secretary of the Attorney-General's Department, to act as a means to bring cyber capabilities across government together (virtually, rather than physically), to strengthen reporting to government.
- Develop strategies to enhance cyber cooperation with the US.
- Establish a cybersecurity dialogue with China.
- Develop a cyber regional engagement strategy for ASEAN Regional Forum countries.

These measures will push Australia rapidly towards a strengthened cyber policy development capability to complement our national cyber operational capabilities.

## Notes

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

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

[3] 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.