POLICY ANALYSIS ASPI

ASPI
AUSTRALIAN STRATEGIC POLICY INSTITUTE

Connecting the docs: towards an integrated national security strategy

by Carl Ungerer

53

10 December 2009

The all-hazards concept of national security is a relatively new one for Australia. Throughout the Cold War, Australian strategic concepts tended to be bounded by traditional calculations of conventional military threats and responses, seen mostly through the prism of alliance solidarity. The core national interests of survival and territorial integrity drove all other security considerations.

As the threat of global nuclear war between the superpowers receded, some predicted a 'new world order' in which states would cooperate rather than compete. But the loosening of structural constraints at the global level had a number of unintended consequences. Competition among and between sub-state groups (ethnic, religious, extremist, cultural or a combination of these) led to greater conflict and violence: sometimes expressed formally through war (as in the former Yugoslavia), but more often expressed through the informal violence of terrorism.[1] The security environment was further complicated by shifts in economic power and influence as well as advances in communications and technology which opened up new pathways for transnational criminal networks to ply their cargo of drugs, people or weapons.

The increasing globalisation of violence meant that Australia's geostrategic isolation was no longer an effective barrier to these sources of transnational insecurity. For example, long before the Australian intelligence community knew its name, the leadership of the Southeast Asian terrorist group *Jemaah Islamiyah* (JI) had nominated Australia as an important base for financial operations. Several JI terrorists visited Australia as tourists. So, in addition to the 'old' strategic concerns about shifting power balances in the Asia–Pacific region, governments in Canberra needed to recalibrate national security policies in order to accommodate this 'new' security environment.[2]

For Australia, responding to the combination of 'old' and 'new' security dilemmas has meant rapid increases in government spending for *both* traditional military capabilities and new transnational security structures. Cumulative Commonwealth government spending on national security initiatives since 2001 (excluding Defence) will reach $10 billion by the end of the decade. And the 2009 Defence White Paper, *Defending Australia in the Asia Pacific Century: Force 2030*, posits a more muscular maritime strategy that will cost in the vicinity of an additional $130 billion over the next twenty years. As a result, 1 in 6 Commonwealth public servants now work on national security related issues.

Despite a widening agenda, and the rapid growth in spending across the national security community, disagreement continues over which issues should be afforded a higher priority and why. And there is, as yet, no formal mechanism within government for deciding whether the current allocation of national security funding—in which the Department of Defence receives the lion's share—is the most effective, cost-efficient or appropriate. So implementing a comprehensive, risk-informed approach to strategic planning remains a high priority.

The elevation of national security issues across many aspects of government policy, and the growth of public sector agencies involved in policy delivery has made the national security agenda more complicated and complex. The creation of the National Security Adviser's position in 2008, situated in the Prime Minister's department, was designed specifically to bring greater coordination to the national security task and to build a more 'cohesive culture' across the whole policy community. But, as the number of moving parts continues to grow, finding common ground between them has become increasingly difficult.

Such complexity is evident in the number of current policy reviews and commissions of inquiry into various aspects of the national security agenda (see Table 1, p.9). In addition to the December 2008 National Security Statement to Parliament, the government has initiated three major White Paper processes (Defence, Counter-Terrorism and Energy Security), conducted multiple policy reviews (homeland and border security, policing and intelligence, cyber security and biosecurity) and released several other policy framework documents (counter-radicalisation, science and innovation, energy security and legal reforms).

Each of these documents is meant to speak to a particular aspect of the national security agenda or to solve a particular puzzle. And each is designed to be subordinate to the general principles laid out in the National Security Statement. But there are still several tensions between the various strands of the overall policy framework.

The internal/external divide

The assertion made by some security analysts and policymakers—that there is no longer a sensible distinction to be made between internal and external security and between domestic and foreign policy—is not matched by the current processes of government. The intelligence community is a case in point. As the principal source of advice to government on new and emerging security risks, the six agencies of the Australian Intelligence Community remain separated by some hard barriers. Overseas and domestic collection is mandated to different agencies. Strict legislative and regulatory controls ensure that such barriers are not crossed.

But this system seems incompatible with the requirement to understand and defeat polymorphous and networked risks such as cyber security, transnational terrorism or state espionage. In deciding on the balance between privacy concerns and the growing interconnectedness of foreign and domestic security threats, governments need to ask if current arrangements are appropriate and tenable.

Vulnerabilities that are simultaneously global and local are met with a series of *ad hoc* policy responses based on the rigidities of this model. The reactive approach to national security legislation is just one example of this. Despite rapid funding growth and a commitment to reform, Australia's bureaucratic structures designed to deal with Cold War security threats have so far survived the new security environment without suffering extensive damage.

Cops vs. spies

A second major debate of the post-Cold War security environment has concerned the connection between the functions of intelligence and policing agencies. In Australia, the lack of formality in exchanges between domestic security intelligence and the police was identified by the 2007 Street Review as a major impediment to national security following the unsuccessful prosecution of a local terrorism suspect.

However, the problem is one that is not unique to local circumstances. Several years ago, a RAND study of counter-terrorism arrangements in Australia, Canada, France and the United Kingdom found that the culture of mistrust and lack of communication between intelligence and police was a serious weakness in efforts to combat the local and global dimensions of the terrorist threat.[3] In some cases, agencies were found to be working at cross purposes—the product of old habits and traditional turf wars.

Recent efforts to formalise working relationships, and to build better habits of dialogue and trust (such as the National Counter-Terrorism Protocol) have improved the overall mechanics of operational cohesion. And there is a much greater sense of 'fusion' between intelligence and overseas military operations. But some problems remain entrenched. In the words of the 2008 Smith review into homeland and border security, ‘some legislative, technical and cultural barriers to information sharing—within and between governments and the private sector—remain’.

Shifting from a strict ‘need-to-know’ principle to a culture of information sharing and public consultation is recognised as an important step towards a more agile and efficient national security community. But the structural impediments that remain in place—including the current hierarchy of security clearances and the incompatibility of information technology systems between various agencies—will continue to frustrate the goal of a more seamless and ‘cohesive’ community.[4]

The diplomatic drought

A third tension in the government’s policy framework concerns the balance and emphasis between military and non-military instruments of national security policy. A notable gap in the current schedule of government white papers is the foreign affairs and trade portfolio. The proposed Foreign Policy Statement to Parliament has not yet materialised. And it has been more than four years, and a change of government, since the last White Paper on Australia’s overseas aid program was written. Given the centrality of diplomacy and development to national security, new policy statements in both areas are needed.

In the United States, senior military officials have called for a major reinvestment in diplomacy and development assistance as the cornerstone of national security policy. In 2008, US Secretary of Defense, Robert Gates, argued that America faced a ‘creeping militarisation’ of foreign policy if more resources were not devoted to the civilian agencies relative to the funding received by the military.

In Australia, the chronic underfunding of the Department of Foreign Affairs and Trade (DFAT) over the past two decades has been well documented.[5] And further downward pressure on DFAT’s budget will only contribute to arguments that the government is less serious about utilising the full range of instruments available to deal with national security challenges. However, a fully integrated national security policy will require investment in both the coercive and persuasive elements of national power—making distinctions between them is pointless. Again, as Robert Gates has acknowledged, the lines separating war, peace, diplomacy and development have become increasingly blurred.

The case for an integrated approach

Having rejected the US model of a Department of Homeland Security in which most bureaucratic elements of the national security community would be brought together under one roof, the creation of the National Security

Adviser’s position was meant to be the connective tissue that joined the community together and provided leadership. But a more integrated national security policy will require greater cohesion among the various strands of activity than one position can manage.

The effective management of emerging risks requires governments to make difficult choices between competing interests, and to foster a more informed public consensus of what actually constitutes a serious risk in the new national security environment. But priority setting in national security planning is increasingly difficult. The number of potential or emerging national security risks is so large that governments cannot address all of them simultaneously. Moreover, priority setting can become captive to the actions of interest groups, the media or public opinion. For example, any rational examination of threats to Australia would rank people smuggling and irregular migration as very low risks to national security. And the identification of risk always contains a subjective political element that governments will seek to exploit.

So the contemporary problem for government is how to assess, prevent, mitigate and respond to the new security environment with the key instruments of national security policy distributed across multiple agencies and jurisdictions. The problem here is that, while the threat environment is networked and multi-faceted, government operates with a structure that is still compartmentalised and based on a division of labour designed to respond to the relatively predictable patterns of the Cold War, but is consistently wrong footed by the new risk environment. In a globalised world, we need as Philip Bobbitt suggests, to ‘think in terms of the interconnectedness of threats, of mitigation instead of fortress defense, of reconstitution instead of retaliation’.[6]

So what would an integrated national security strategy look like? It would first need to acknowledge that the national security agenda is not fixed but one that varies over time. Risks that are interconnected such as cyber security and terrorism can have cascading consequences, often rendering a comprehensive understanding of the scale of a crisis beyond the competency of a single agency or arm of government. Such events have been described as ‘outside the box’, ‘too fast’ and ‘too strange’.[7]

Mechanisms must therefore be found for identifying and incorporating new and emerging risks into national security planning without compromising the existing security structures. Horizon scanning or strategic forecasting plays an increasingly important role in the planning assumptions of key allies such as Singapore, Canada and the United Kingdom, but remains an under-resourced and therefore under-valued element of the Australian national security effort. The immediate introduction of a dedicated and well-funded horizon-scanning capability at the heart of the national security establishment should be a top priority for government.

Second, a fully integrated national security strategy would have the agility to arrive at a comprehensive understanding of risks on an all-hazards basis and to allocate funds to those priorities in a timely and effective manner. Although work towards a single national security budget has started, such efforts will only be useful if they can move funding between and within agencies in response to changes in the security environment. But such a change is not being contemplated. It would require a fundamental reorganisation of government budgetary processes, to the extent that individual agencies and Ministers could lose the ability to decide how and when portfolio budgets were spent.

Finally, a national security strategy should be built around a single conceptual framework. This is important for ensuring a commonality of effort and clear policy direction. Indeed, the National Security Statement explicitly acknowledges the need for ‘a new concept of national security capable of embracing and responding to the more complex and interconnected operating environment that we will face for the future’.

At various stages in our history, previous governments have attempted this: the 1989 ministerial statement *Australia’s Regional Security* was guided by notions of ‘multidimensional’ security; the Keating government introduced the concept of ‘cooperative’ security in the mid-1990s; and the Howard government framed its foreign and strategic policy calculations within the broad rubric of the ‘national interest’.

Currently, there are several conceptual frameworks driving the government’s national security agenda—some of them are not entirely consistent with the others. For example, the National Security Statement identifies seven key principles: defence self-reliance; strengthening alliance relations with the US; regional engagement; commitment to multilateral institutions; creative middle power diplomacy; risk-based planning; and partnership with state and territory governments. Each of those could be an organising principle for a national security strategy—in combination they tend to confuse more than they illuminate.

For example, the 2009 Defence White Paper has sought to return Australian strategic concepts to their ‘classical’ roots of self-reliance and geographical primacy. But, as the National Security Statement makes clear, ‘the government’s approach to national security encompasses more than just traditional statecraft or classical military capabilities’. The government has so far resisted giving this dualistic strategy a formal title—but the conceptual approach is not dissimilar to the Japanese notion of ‘comprehensive’ security, in which an explicit attempt is made to balance foreign and domestic security concerns.

The concept that is better suited to the current environment is ‘networked security’. A network is a complex system of individual elements. A network can be formally constituted or created online as a virtual community. It can be formed, funded and disbanded as needs arise. The network model acknowledges that current national security threats are interconnected and unlikely to be solved through the actions of one agency, one policy decision or one country acting alone.

A networked strategy would involve building inter- and intra-governmental teams around a set of identified security risks and would incorporate advice from the private sector and the wider policy community. Internationally, it would privilege ‘like-minded’ coalitions of countries to address specific security problems. In practice, it would bring national security priorities and funding into closer alignment by addressing issues from a more holistic, whole-of-government perspective.

Conclusion

Unlike in the US, the concept of national security in Australia is not yet deeply embedded in the psyche of the modern state. The US gave the term currency during the Cold War as a means of articulating a vision for universal democratic transformation. For the most part it meant ‘the threat, use and control of military force’ in defence of national territory and political institutions.[8] And it involved a limited range of policy instruments: military force, intelligence and diplomacy.

The contemporary national security challenges for Australia are of a different order of magnitude. The range and complexity of risks—from an unconventional war with a major regional competitor to the threat of homegrown terrorism—compels modern governments to take a more comprehensive, strategic approach to national security planning.

The National Security Statement and the number of policy reviews across the national security agenda have provided a much needed foundation on which to build a new security paradigm. The next challenge for government is to bring these elements of public policy together into a single, coherent framework. To that end, the next iteration of the National Security Statement to Parliament should be elevated to a strategy document, similar in scope and ambition to the Defence White Paper process. Properly resourced, such an undertaking should not take more than twelve months to complete. And it would benefit from having a dedicated writing team working outside existing departmental structures.

The centerpiece of the strategy paper should be a national risk assessment. Like current efforts in Canada, the United Kingdom, Singapore and Germany, risk assessments are used to provide governments with a clearer picture of the national risk profile and to capture the range of emergencies, both natural and malicious, that might have an impact on security. Risk assessments are needed to gauge the likelihood and consequences of any national emergency. An important analytical goal is to describe the scale, extent and connectivity of emerging threats and to identify strategies for effective remedial action.

On the basis of a national risk assessment, the government should identify 3–5 of the most serious and immediate priorities for Australian national security and build networks across the national security community to deal with those problems. This approach has a number of advantages: it acknowledges that governments have limited resources to deal with all national security risks (and that some risks are tolerable); it creates a networked, whole-of-government effort across all jurisdictions; it is adaptable and flexible; and it is measureable—it allows you to set specific targets for outcomes.

For Australia, building a networked national security strategy based on a comprehensive assessment of risks and responses would require a fundamental change in current processes and thinking. But it is a change that is both necessary and overdue.

Table 1: National Security Policy Reviews

Review	Announced / Conducted by / Agenda	Outcome
Homeland and Border Security Review (Smith Review)	Announced: 22/2/08 Department of Prime Minister and Cabinet Consider the roles, responsibilities and functions of departments and agencies involved in homeland and border security.	Report released: 27/6/08 Recommendations addressed in Prime Minister Rudd's National Security Statement 4/12/08
National Security Statement	Office of National Security, Department of Prime Minister and Cabinet	Released: 4/12/08 Under periodic review
Defence White Paper 2009	Announced: 22/2/08 Department of Defence Defending Australia in the Asia Pacific Century: Force 2030.	Released: 2/5/09
Quarantine and Biosecurity Review	Announced: 19/2/08 Quarantine and Biosecurity Review Panel, chaired by Roger Beale	Report released: 18/12/08 Australian Government's preliminary response, September 2008, which agrees in principle with all 84 of the review's recommendations, subject to Budget processes.
The Street Review: A Review of Interoperability Between the AFP and its National Security Partners	Announced: 22/11/07 Committee: Sir Laurence Street, Martin Brady and Ken Moroney	Report released: 12/3/08 All 10 recommendations accepted by the AFP
Whole of Government Review of E-Security	Announced: 2/7/08 Attorney-General's Department Development of a new e-security framework for the maintenance of a secure and trusted electronic environment for both public and private sectors.	Report Released: 19/12/08 Recommendations accepted National computer emergency response team (CERT) in Attorney-General's Department set-up Cyber Security Strategy released on 23 November by Attorney-General
National Energy Security Assessment (NESA)	Announced: 2007 election campaign and in National Security Statement Department of Resources and Energy. Strategic energy security issues in the liquid fuels, natural gas and electricity sectors currently, and those likely to influence the level of energy security in 5 years to 15 years (2023).	Report released: March 2009 Findings of this report feed into future energy-related policies and the Energy White Paper expected later this year

Inquiry into the legislative arrangements to outlaw serious and organised crime groups	Review announced 17/3/08 Parliamentary Joint Committee on the Australian Crime Commission	Report released: 17/8/09 Report or government response to inquiry not yet released *
Inquiry into the National Security Legislation Monitor Bill 2009	Announced 25/6/09 Senate Finance and Public Administration Committee Inquiry into establishing a monitor of Australia's counter-terrorism and national security legislation.	Report past due: 7/9/09 In progress
Inquiry into Nuclear Non-proliferation and Disarmament	Announced: 13/10/08 Joint Standing Committee on Treaties Inquiry into role of treaties and how government can contribute to non-proliferation and disarmament.	Report released: 17/9/09 22 recommendations Government response to inquiry not yet released *
Security at military bases	Announced: 5/8/09 Chief of the Defence Force Angus Houston Inquiry into the practice of using private security firms to guard military installations.	Report released: 19/10/09 Actions are either complete or in progress on all recommendations
Inquiry into the Anti-Terrorism Laws Reform Bill 2009	Review announced: 25/6/09 Senate Legal and Constitutional Committee Inquiry into amendment of the following Acts: Criminal Code Act 1995, Crimes Act 1914, Australian Security Information Organisation Act 1979 and repeal of National Security Information Act 2004	Report released: 28/10/09 Report or government response to inquiry not yet released *
National disaster resilience strategy	Review announced: November 2008 Attorney-General's Department and Emergency Management Australia Commissioned by the Ministerial Council for Police and Emergency Management (MCPEM) To produce a National Catastrophic Natural Disaster Plan and action plans.	In progress
National Security Science and Innovation Strategy	Department of Prime Minister and Cabinet	Strategy launched 24/11/09

Inquiry into Cyber Crime	Review Announced: 13/5/09 House Standing Committee on Communications Nature and incidence of cyber crime in Australia	In progress
Lexicon of Terrorism Project	Announced: 6/7/09 Attorney-General's Department Examine the use of language by Commonwealth, State and Territory Governments' in relation to terrorism.	In progress
Counter-terrorism White Paper	Announced: in National Security Statement, 4/12/08 Department of Prime Minister and Cabinet, Office of National Security	In progress

* = No government response or report on inquiries recommendations located

Endnotes

1 These judgements were central to ASIO's 1995 strategic assessment. See ASIO, *Report to Parliament 1995-96*, Canberra, 1996, p. 3.

2 See David Martin Jones and Susan Windybank, 'Between two worlds: Australian foreign policy responses to new and old security dilemmas', CIS Occasional Paper 97, October 2005.

3 Peter Chalk and William Rosenau, *Confronting the"“enemy within”: security intelligence, the police and counterterrorism in four democracies*, RAND, Washington DC, 2004.

4 See ASPI *Policy Analysis 51, '*Information sharing in Australia's national security community' by Kelly O'Hara and Anthony Bergin http://www.aspi.org.au/publications/publication_details.aspx?ContentID=232&pubtype=-1

5 Lowy Institute for International Policy, *Australia's Diplomatic Deficit: Reinvesting in our instruments of international policy*, http://www.lowyinstitute.org/Publication.asp?pid=996, Sydney, March 2009.

6 Philip Bobbitt, *The Shield of Achilles: War Peace and the Course of History*, London, Penguin 2002, p. 793.

7 P. Lagasec, 'Crisis: a watershed from local, specific turbulences to global, inconceivable crises in unstable and torn environments', paper presented to the conference *Future Crises, Future Agenda – An Assessment of International Crisis Research*, France, 2004.

8 Stephen Walt, 'The renaissance of security studies', *International Studies Quarterly*, 35(2) 1991. pp. 211-39.

About the Author

Dr Carl Ungerer is Project Director of ASPI's Australian National Security Project.

About Policy Analysis

Generally written by ASPI experts, **POLICY ANALYSIS** is provided online to give readers timely, insightful opinion pieces on current strategic issues, with clear policy recommendations when appropriate. They reflect the personal views of the author 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