POLICY ANALYSIS ASPI

ASPI
AUSTRALIAN STRATEGIC POLICY INSTITUTE

57

# Homeward bound: Australia's new Counter-Terrorism White Paper

by Anthony Bergin and Carl Ungerer

18 March 2010

The February 2010 release of the Rudd government's Counter-Terrorism White Paper: *Securing Australia – Protecting our Community,* is an important milestone in Australia's evolving national security policy framework.

The release of the White Paper follows the announcement of a series of major initiatives on cyber-security (November 2009), the release of the National Security Science and Innovation Strategy (November 2009), the Defence White Paper (May 2009), and the Australian National Security Statement (December 2008).

Fourteen months after it was first proposed in the National Security Statement, the Counter-Terrorism White Paper has been generally well received. Most media coverage, however, has focused on a key 'announceable' of the paper; the investment of $69 million to introduce biometric-based visa systems in ten countries to reduce the risk of terrorists, criminals and other persons of concern entering Australia undetected.

The list of ten countries has not been released publicly, although media reports have suggested that Pakistan won't be included. That would be a puzzling omission if true: the White Paper correctly identifies Pakistan (and Afghanistan) as of the 'greatest concern' globally when it comes to the potential spread of politically motivated violence. Indeed, Pakistan remains a central training ground for terrorists.

Stepping back from the issue of biometric screening, it's important to ask a set of broader questions about the strategy and policy in the White Paper: In what ways does this document represent a shift in government thinking on the nature and direction of the terrorist threat to Australia; what did it miss; and how will Australia's counter-terrorism strategy evolve to achieve the government's stated aim of protecting Australia, its people and interests from terrorism? This *Policy Analysis* offers some ideas on the elements of a more comprehensive counter-terrorism strategy.

## A growing new threat

For several years now, analysts have been charting a global shift in terrorism away from previously hierarchical organisations such as al-Qaeda and Jemaah Islamiyah towards smaller, looser networks of amateurs inspired by al-Qaeda's violent rhetoric, but who may not have any direct operational or financial linkages to a known terrorist organisation.

Marc Sageman, Senior Fellow at the Foreign Policy Research Institute, is the most well-regarded analyst of this kind of 'self starter,' homegrown terrorist phenomenon. He has argued that the future terrorist threat will be driven by 'bunches of guys' who have become radicalised by Salafist or Wahabist ideologies, but who remain self-motivated and 'leaderless'. The involvement of medical practitioners in the failed car-bomb plot in London, the attack on Glasgow International Airport in 2007, and a lone Nigerian student's failure to ignite a bomb in his underpants on a flight to the United States on Christmas Day 2009 give some indication of the amateur tradecraft of these types of individuals.

That's not a reason for complacency, however. On 22 February this year, Najibullah Zazi, a 25-year-old Afghan and legal resident of the United States for ten years, admitted that he had had explosives training in Pakistan. He was to use his training in a planned suicide attack in New York City. He also pleaded guilty of provision of material support to al-Qaeda.[1] In the aftermath of the guilty plea the US Attorney General stated that the plot would have been 'deadly' had it succeeded.

The core judgment at the heart of the Rudd government's Counter-Terrorism White Paper is that, although homegrown extremists haven't launched a successful attack here, we are no longer immune from domestic cells prepared to move from violent rhetoric to action: indeed, we face a permanent and persistent threat from enemies both inside and outside the country.

The White Paper notes that although more than one hundred Australians have been killed in terrorist attacks overseas, thirty-eight people have been prosecuted on terrorism-related charges in Australia, most of them since 2005. It also expresses concerns about the possibility of Australians travelling to places such as Somalia and Pakistan to train and then conduct terrorist attacks inside Australia.

The sobering message in the White Paper is that, while we have a good track record of achievements in countering terrorism, our holiday from terrorism is over. We're now learning what the populations of the United Kingdom and other countries such as Indonesia have known for some time: terrorist violence against their citizenry can be perpetrated by their own legal residents or citizens.

That assessment moves the national debate on terrorism some distance from the 2004 counter-terrorism White Paper, which placed more emphasis on keeping dangerous people and goods out of the country. Interestingly, though, the language hasn't changed that much in six years. The Howard government's White Paper described the principal threat to Australia as coming from 'extremist-Muslim terrorism'. And Foreign Minister Downer talked openly about 'Islamo-fascists'.

Despite the current federal Attorney-General last year backing a project to ensure that governments describe terrorism in a way that doesn't alienate Muslim communities or inadvertently glorify terrorism, the White Paper adopts the term 'jihadist' terrorism. It notes, however, in a footnote that the term is an 'imperfect descriptor' with 'multiple' meanings.

Some commentators have been quick to denounce the use of this language, arguing that adopting this term does more harm than good; it risks giving terrorists the religious legitimacy they seek and reinforces the idea that we are somehow at war with Islam.[2]

But it's almost impossible to describe the movement that's been responsible for terrorist attacks from New York to Jakarta to London without causing offence. All those involved in these attacks have had an Islamist political agenda. And they believe that this should be achieved through violent 'jihad' or struggle.

The new White Paper acknowledges the continuing threat of al-Qaeda's organisational reach in Afghanistan and tribal parts of Pakistan, and its growing tentacles in North Africa, particularly Yemen and Somalia (where training programs run by al-Shabab have attracted hundreds of extremists from around the world).

The White Paper usefully reminds readers that, despite some tactical successes in Afghanistan and Pakistan, al-Qaeda is reviving its base: its leadership 'still has a substantial pool of operatives capable in their own right of planning and conducting attacks and helping other like-minded extremists across the globe'.

There's a clear attempt in this White Paper, however, to rebalance community threat perceptions. Terrorism is now just one of a number of national security risks and pressures that governments must face. It's described as a 'persistent and permanent' feature of the national security environment. In this way the White Paper usefully reminds us that there's no such thing as absolute security and that trying to achieve it will prove counterproductive. Overall, these judgments represent a maturing of the counter-terrorism debate in Australian politics.

The White Paper doesn't shy away from the global ideological threat from jihadist groups. It acknowledges that the scale of the problem is directly related to the size, composition and social inclusiveness of migrant Muslim populations in Western societies. Importantly though, the strategy usefully explains how the measures the government is taking to detect and prevent terrorism should always seek to be lawful, proportionate and uphold democratic ideals.

It's hoped that security officials communicate this aspect of the new strategy so that counter-terrorism measures alert, rather than alarm the public.

## A new strategy

Media reporting on the White Paper has missed a fundamental aspect of the document – the change in strategy. Without fanfare, the Rudd government has re-cast the four major elements of our counter-terrorism strategy from *prevention, preparedness, response and recovery* to the slightly more ambiguous *analysis, protection, response and resilience*.

The previous approach was at the heart of the federal–state agreement on domestic counter-terrorism policy following the creation of the National Counter-Terrorism Plan in 2005. The work of the states and territories in each of these four streams will now need to be reviewed and possibly revised.

*Analysis* is an activity that underpins all four components of the strategy. This is quite different from the previous White Paper's focus on *prevention*, although it's possible the term *analysis* was adopted to emphasise to the wider community that all aspects of our counter-terrorism efforts are intelligence led and evidence based.

The creation of a new Counter-Terrorism Control Centre to be located in ASIO is touted as the focal point for the new intelligence-led analysis of the terrorist threat. But it's not clear that another layer of bureaucracy will necessarily improve the flow of information beyond existing arrangements.

A more effective approach for sharing terrorism information may be to harness Web 2.0, which utilises the internet as an effective communication tool for improving knowledge and fostering collaboration. The US intelligence community has created Intellipedia, a Wikipedia-style portal for information sharing, and A-Space, a MySpace equivalent for intelligence analysts to connect with colleagues working on similar topics.

Much of the old *prevention* agenda, including public awareness campaigns, and border and aviation security, has been subsumed under the *protection* stream.

This element of the strategy is more about capability planning than a proactive, risk-informed approach to preventing terrorism.

Although there's some overlap in each element of the strategy, the *resilience* agenda in the new White Paper is a marked difference from the previous *recovery* stream; the coordinated process of economic, environmental, physical and community recovery in the face of a disaster—whether manmade or natural (see discussion below).

## Where are the metrics?

At just seventy-one pages, the White Paper is concise (the equivalent UK document is over one hundred pages longer). And the $69 million funding initiative on aviation security measures is found in one small paragraph in the concluding chapter**.** To put this funding announcement into perspective, the 2009 Defence White Paper committed over $130 billion in new defence spending over the next twenty years.

To be fair, cumulative government spending on counter-terrorism since 2001 has reached around $10 billion, and will naturally taper off. In some respects it's reasonable to argue that we have over-concentrated on intelligence resources: the bulk of this investment has seen the Australian Intelligence Community expand four-fold.

Our counter-terrorism measures should be undertaken at an acceptable cost in dollars, lives and other national policy priorities. Terrorists evaluate operations after they are carried out in order to learn from them. As the White Paper itself points out, terrorist groups have proven 'highly adaptable' and have the 'capacity to learn from their mistakes.' But very little of the $10 billion dollars Australia has spent on counter-terrorism over the last nine years has been used to evaluate the effectiveness of the measures undertaken against terrorism.

This is a notable omission from the White Paper. Unlike the British counter-terrorism strategy, *Contest Two,* released last year, the Australian White Paper is silent on how the government's strategy will be monitored and measured.

This is surprising. Overall, there's been a much stronger push under the Rudd government to bring national security into line with the standards of performance evaluation across the public sector. The new risk-informed approach to national security budgeting and planning gets little mention in the White Paper.

Under extensive performance management guidelines, the *Contest Two* strategy identifies a number of performance benchmarks, including the extent and quality of intelligence information, the disruption of potential threats and the timeliness of ongoing vulnerability assessments around hazardous sites and crowded places. Each of the four elements of the British strategy (*pursue, prevent, protect, prepare*) has a detailed delivery plan, including projected timelines, benefits and costs.

For Australia, important metrics will include the disruption of terrorist attacks on home soil and the extent to which government policies can prevent linkages between individuals radicalised at home and transnational terrorist organisations that might seek to exploit them. The White Paper identifies terrorist groups in Somalia, Yemen and Lebanon as emerging concerns (with Pakistan cited as an ongoing problem), highlighting the reality that the global threat is ideologically malleable and geographically promiscuous.

## Down to business

There's also a blind spot in the White Paper in relation to business. The only real mention of the contribution of the private sector to counter-terrorism efforts is around asset protection. The paper notes that, as the owners and operators of infrastructure may be targeted by terrorists, the business community has a key role to play in Australia's response to terrorism. That's a fair judgment: the vast majority of Australia's critical infrastructure is in the hands of the private sector.

But there's no recognition in the paper of the role, responsibility and capability of private security firms at both industry and professional levels. At the industry end there are approximately the same number of licensed security guards as police and regular military personnel combined. Private security is responsible for the initial detection, deterrence, delay and response at almost all critical infrastructure.

The security industry is a critical element in information gathering and can provide intelligence through their knowledge of operating environments and communities. It's disappointing the White Paper fails to acknowledge that it is corporate sector professionals who will in many cases develop, implement, test and fund the ability for Australia to survive a security incident.

The White Paper might have suggested here, for example, that in order to maximise access to relevant security technologies and services, a national customer group should be established that brings together key Australian government agencies to develop and discuss broad capability requirements. This could be discussed with a newly formed industry peak body, the Australasian Council of Security Professionals.

And Australia might also adopt a version of Project ARGUS, an initiative of the UK National Counter Terrorism Security Office. This initiative explores ways to help business prevent, manage and recover from a terrorist attack. It achieves this by taking businesses through a simulated terrorist attack. The simulation, on a DVD, identifies the best way to implement the terrorism management strategies mentioned above.[3]

And finally, when it comes to the private sector and infrastructure, the White Paper fails to recognise that the critical foundations that underpin our society are deteriorating, and that there are associated risks. The 2010 Infrastructure Report Card released in early March by Engineers Australia rated all infrastructure in Victoria as barely adequate.[4] The upkeep of critical infrastructure is a sound national security measure: it removes the kinds of vulnerabilities that terrorists might be tempted to target or exploit.

## Resilience

The use of the term *resilience* in the White Paper as a key element in the overall strategy is limiting. The White Paper adopts the term to describe the ability of communities to resist extremist messages. But that's not how the concept of resilience is used by most analysts of national security.

Rather, it's normally understood to refer to creating a community which can prepare, respond and 'bounce back' from emergencies, whether manmade or natural. And when talking about protecting critical infrastructure, resilience means putting in place systems and programs that will ensure that our infrastructure can endure the worst of what man or nature can throw at us.

Most analysts use *resilience* in this 'snapping back' sense, where a system has the ability to absorb change while retaining its essential function, the ability to maintain self-organisation, and the capacity to adapt and learn. Indeed, that's how the term is broadly defined in the December 2009 Australian National Disaster Resilience Statement, issued by the Council of Australian Governments (COAG).

Much of the resilience element of the strategy, in so far as it talks about the role of the community, would probably have been better placed under the *protection* strand of the overall approach.

## Confronting the homegrown threat

Last year, in a speech to ASPI, the Attorney-General, Robert McClelland, laid the groundwork for the government’s approach to combating violent extremism in Australia.[5] And further resourcing measures for a counter-radicalisation strategy may be announced in the 2010–11 budget cycle. But lingering concerns about this White Paper remain: if homegrown terrorism is the problem, what’s the solution?

At this point there are no exact figures on how much we’ve spent on counter-radicalisation related activity. And there were no ‘announceables’ in the paper when it comes to a comprehensive counter-radicalisation strategy.[6] Indeed, there’s nothing in the White Paper on the government’s overall counter-terrorism communications strategy as it relates to our Muslim communities. Government resources are important here, just as in other areas of law enforcement.

Although the White Paper accepts that community engagement is essential in reducing the terrorist threat over time, it appears to adopt the view that because preventing violent extremism is a sensitive matter, it’s best not to spell out what specific measures the government might have in mind. But undue secrecy in practice may serve only to unbalance community relations and reduce the prospect of gaining the broadest possible consent for measures to keep communities safe from radicalising influences.

Fortunately, Australia doesn’t have the mixture of discrimination and alienation in our Muslim communities that exist in Europe, where sub-cultures have allowed extremism to thrive. Nor do we have the concentration of one group, such as the Pakistani community in the United Kingdom. Australian Muslims are much better integrated, and Australians generally accept Muslim immigrants as a welcome addition to the country. Unlike the Swiss, minarets don’t worry us and we aren’t likely to see a movement here anytime soon to ban the burka, as is favoured by the French President.

But Australian government officials at all tiers of government should continue to expand their efforts to reach out to Muslim communities, including the regular attendance of senior political figures at local Muslim festivals and celebrations. Although the White Paper urges vigilance against emerging threats, we must also ensure that Australia’s Muslim communities feel respected and trusted when new counter-terrorism measures are announced.

We want to ensure that we promote a future where young Australians don’t consider joining extremist groups in the first place. It’s disappointing, therefore, that there’s limited recognition in the White Paper of the exploitation of the internet as a conduit for radicalisation or why it’s likely that internet-based recruitment will increase in importance.[7]

There are more than 4,000 terrorist-related websites worldwide. Ideas cross borders through cyberspace. We aren’t going to ban our way out of this problem. Cyberspace affords individuals access and anonymity in an extremist environment and the ability to find like-minded extremists in thousands of chat rooms and social networking sites.

Australian policymakers should make the web a key component of domestic counter-radicalisation, cooperating with the private sector and international partners, not just in monitoring but also enabling our Muslim communities to counter the arguments of extremists.

The UK's Quilliam Foundation, formed by previous members of UK-based Islamist organisations, works with police, Muslim parents and others to debunk radical propaganda and provide a disinfectant against extremist views. Another initiative that may provide lessons for Australia is the United Kingdom's STREET (Strategy to Reach, Empower, and Educate Teenagers) project run by conservative Muslims who have a proven track record in countering violent extremism. The project received an award last year from London Minister, Tony McNulty, in recognition of its work in de-radicalisation.[8]

Moreover, there's no recognition in the White Paper of the role prisons play as proven incubators of radicalisation; many people convert to religious faith in prisons and, in Europe, Islam attracts more converts than other faiths. Radical imams can have access to inmates and Islamist militants can attract recruits inside prison.

As we are now seeing an increasing Muslim population in our prisons, we need to start thinking about how best to develop a strategy for countering radicalisation, heeding the lessons learned in Europe and elsewhere in the implementation of de-radicalisation programs. A new de-radicalisation program will soon be introduced into New South Wales prisons as part of the management plans for inmates convicted of terrorism.[9]

The White Paper sensibly suggests that we consolidate research on violent radicalisation and the factors leading to violent extremism in Australia. Here we should take a leaf out of Norway's book. The Transnational Radical Islamism Project at the Norwegian Defence Research Establishment provides in-depth studies on patterns of radicalisation and recruitment. Australia has no dedicated centre in terms of resources and expertise.

## New movements ahead?

While the White Paper correctly argues that our main terrorist threat derives from radical Islamists, it also notes that:

> In the future new terrorist threats could manifest themselves in Australia, either as a by-product of events overseas or as a result of a political grievance within Australia. There will always be the disaffected and disempowered, often but not always at the fringes of communities or the followers of radical ideologies, who mistakenly see advantages in the use of terrorist tactics.

The White Paper doesn't elaborate here, but two possibilities are realistic. The first might be environmentalists who have on occasions used acts of violence to convey their message (although they have largely restricted themselves to low-level acts of vandalism). Last June there were allegations that the Earth Liberation Front had hand delivered a threat to the house of a power station manager in Victoria.[10] But at this stage it's unlikely we would see environmental groups resort to the type of mass casualty attacks that have been perpetrated by radical Islamist organisations.

The second concern is far right-wing extremism. We have seen such groups emerge in both Europe and the US in response to the global economic downturn. Last year the US Department of Homeland Security issued a warning about the rise of white supremacists and other right-wing extremist groups.[11] In July 2009, a serious right-wing terrorist plot in Britain was uncovered that involved a bombing campaign against mosques.[12] In the future our security and intelligence agencies may need to focus more resources on tackling other potential forms of violent extremism.

## International cooperation

Finally, the White Paper correctly notes that, given the transnational nature of the threat and the willingness of some countries to export terrorism to Australia, we must engage in international cooperation. This poses real challenges in terms of sharing sensitive information, especially in areas that require high degrees of trust. Trust only emerges in established relationships; Australia has rightly pursued international counter-terrorism cooperation on a predominantly bilateral basis, establishing counter-terrorism framework agreements with fourteen countries.

Australian efforts to promote security cooperation through multilateral institution building in Southeast Asia have enjoyed less success. The six-nation Multi-National Operational Support Team (MNOST) based in Jakarta has now collapsed. And despite improvements in security cooperation in other areas such as bomb data analysis and forensic work, sub-regional police coordination will require further investments in both training and equipment.

## Concluding remarks

Under the Howard government, counter-terrorism strategy focused almost exclusively on preventing terrorist threats from reaching the Australian homeland: there was a strong emphasis on the US alliance, the Bush Administration's 'war on terror' and border security.

Although the Rudd government's strategy acknowledges the need for international action and a comprehensive, layered approach to national security, there's now a greater political, although not as yet financial, emphasis on tackling violent extremism at home by working with Muslim communities across Australia.

The new strategy represents months of hard work and is the product of broad consultations involving government agencies, law enforcement professionals and external experts. Let's hope that the new direction in the White Paper towards countering homegrown extremism gains the broadest possible support in helping reduce the threat of terrorism in our country.

### Endnotes

[1] AG Sulzberger & WK Rashbaum, 'Guilty plea made in plot to bomb New York subway', *New York Times*, 22 February 2010.

[2] D Flitton, 'Calling them jihadist helps the terrorists', *The Age*, 24 February 2010.

[3] See http://www.nactso.gov.uk/argus.php.

[4] See http://www.engineersaustralia.org.au/irc.

[5] R McClelland (Attorney-General), 'Speech to the Australian Strategic Policy Institute', 21 July 2009, http://www.attorneygeneral.gov.au/www/ministers/mcclelland.nsf/Page/Speeches_2009_ThirdQuarter_21July2009-SpeechtotheAustralianStrategicPolicyInstitute.

[6] For ideas on counter-radicalisation strategies, see A Bergin, *Contest Two and counter-extremism: lessons for Australia*, ASPI Policy Analysis, 2 June 2009, http://www.aspi.org.au/publications/publication_details.aspx?ContentID=216&pubtype=9.

[7] See RSIS–ASPI joint report, *Countering internet radicalisation in Southeast Asia*, Special Report, 6 March 2009, http://www.aspi.org.au/publications/publication_details.aspx?ContentID=202&pubtype=10 and ASPI Strategic Policy Forum, *Countering online radicalisation in Australia*, 13 July 2009, http://www.aspi.org.au/research/spf.aspx?tid=9

[8] Lambeth Council, *Community safety project scoops prestigious award*, media release, 18 February 2009, http://www.lambeth.gov.uk/NR/exeres/1403FE55-885D-4D21-BEB3-C492A146E907.htm

[9] 'Terrorists to be "de-radicalised" in NSW supermax', *ABC News*, 25 February 2010, http://www.abc.net.au/news/stories/2010/02/25/2829559.htm.

[10] B Doherty, 'Eco-terrorists threaten Hazelwood power station boss, *The Age,* 16 June 2009, http://www.theage.com.au/national/ecoterror-threat-sparks-law-review-20090615-carn.html

[11] US Department of Homeland Security, 'Rightwing extremism: current economic and political climate fueling resurgence in radicalization and recruitment', Office of Intelligence and Analysis assessment, 7 April 2009, http://www.fas.org/irp/eprint/rightwing.pdf.

[12] V Dodd, 'Police fear far-right terror attack', *Guardian*, 6 July 2009.

## About the Authors

**Anthony Bergin** is Director of Research Programs at ASPI.

**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