POLICY ANALYSIS ASPI

ASPI
AUSTRALIAN
STRATEGIC
POLICY
INSTITUTE

32

Communicating risk: Revising Australia's counter-terrorism alert system

by Anthony Bergin

31 October 2008

The Attorney-General, The Hon Robert McClelland, announced on 30 September 2008, the implementation of a new national counter-terrorism alert system, arguing that the existing system could be expensive and onerous for communities not directly affected by a terrorist event.

He described the current national alert system, that communicates an assessed risk of terrorism to Australia, as requiring a 'one in, all in' approach across the nation: if an alert level was changed for one part of the country or sector, it would change for all.

Improving Australia's terrorism warnings

From 1 October 2008, the range of four alert levels (low, medium, high, extreme) will remain the same; but compared to the old system, there's a difference in how they will be applied. While an alert level may be declared nationwide, it can now apply to a specific industry, business sector or geographic location.

This more targeted, fine-grained approach is certainly a more efficient and cost-effective system, particularly for business. The previous, overly general approach, (the fourth level of 'extreme' was added in June 2003, to replace the three-level system which had been in use since 1978), has resulted in businesses not directly threatened having to incur the expense and disruption of invoking emergency protocols.

The single national system, indicating the current general level of threat, never made much sense in a country the size of Australia. It resulted in difficulties in providing timely information on the type of incident, location, and the time period of the threat to business, and local and state governments. And it has confused the public: since 12 September 2001 Australia has been on medium level alert, which means that a terrorist attack within Australia could occur at anytime.

Our officials have been reticent about changing the alert level in the absence of specific threat intelligence. The Bali bombings, (October 2002), the Madrid train attacks (March 2004), the Australian embassy bombing in Jakarta (September 2004), and the London bombings (July 2005) did not trigger a change in the national alert level.

The public have therefore been left to wonder about the value of the threat level system. This concern has been underlined when they have seen levels raised at various times overseas, and where specific sectors such as mass transit or aviation have been widely perceived by the public (and talked up by the media) as attractive targets at home.

Comparative approaches

Our broad four-level alert system is similar to the US approach, albeit with two important differences. We use plain words, not colour coding and we have defined risk solely in terms of the probability of a terrorist attack. The US system defines risk in terms of both probability and severity. The US alert system has suffered from problems relating to the public's perception of credibility. The pattern over several years of raising and lowering alert levels, (since 2002, the United States went to orange alert—high risk of terrorist attack—eight times), and the appearance on several occasions that the system was subject to political manipulation, has led to a public becoming cynical and somewhat distrustful of government warnings.

The UK threat level is publicised in several ways, including through the Home Office and MI5. Threat levels are assigned nationwide, to particular regions, and to economic sectors. These levels, (critical, severe, substantial, moderate, low), are communicated to government, police and companies with responsibility for critical infrastructure protection. Until 2006, British authorities announced threats to the public only when there was specific actions members of the public could take to defend themselves. However, for the last two years the general public has also received the information. In practice, the threat level has never fallen below critical or severe (the top two levels) since it was first introduced in 2006 and has been at severe since July 2007.

The Israeli Government, by contrast, takes a different approach: it issues specific alerts to the military and law enforcement agencies, which are sometimes passed on to the media, to inform the public where and when extra vigilance is warranted. Alternatively, France uses a colour coded system which is a four-level pre-established security plan, rather than a warning system, designed to alert the public and motivate action. Each level of the alert requires specific security actions. Similar to France, Spain uses a three-level, tiered (but not colour coded) response plan.

Next steps

No national alert system can tell us precisely what to do. That will always come back to local authorities informing the public what to do in some detail, just as in the case of bushfire danger alerts. And no alert system can deliver perfect security or tell us exactly what we should look for: intelligence is almost never that precise. In the new terror age we need to be vigilant all the time, regardless of the exact alert level in force. And we will rarely know if the alert system works. It's hard to know if a planned attack is aborted due to better security.

The purpose of terror alerts is to deter attacks by making success less certain and to ensure an efficient response if deterrence fails. It's also about preparedness, vigilance and pre-emptive actions. These were defined very loosely for the previous very general, single national alert, and will need to be redefined for the new tailored approach. It's not clear for example whether responses will be identical in every state or territory.

The key question is whether the new changes to the national alert system will help to inform state and territory governments, business and the community plus inform everyone what to do when conditions change. Will it tell us if a threat is serious enough to divert time, money and people from normal activities? And will it assist the public and business (which has invested heavily in protective security and business continuity since 11 September 2001), in knowing how to change behaviour to increase security?

It's not yet clear if the announced changes to the national counter-terrorism alert system will in practice assist in guiding local decision makers, industry and the public on the kinds of protective measures that should be taken at each of the different alert levels.

It's also not clear how individuals will receive public alerts well in advance of a crisis. The new terrorism alert changes should be seen in an all-hazards context: disaster alerts should be brief, simple, clearly worded and take advantage of appropriate technologies. We need to consider adopting a standard emergency warning signal for all hazards and to commit resources to a warning signal which would be consistent nationally. We need to educate the public, when they hear this, to listen and take appropriate action.

Hopefully, the new changes to the terrorism alert system should spur our security agencies to include in the conversation all tiers of government and business, and to develop a set of specific actions, in specific regions, that are available at each level of the alert system. In doing so, however, the critical aspect of timely communication to the public must be a priority. We should invest in ensuring that this important change introduced by the Attorney-General is supported by a robust and consistent communication warning system.

If that happens, then the recent changes will make a valuable contribution to the national security effort.

About the Author

Dr Anthony Bergin is Director of Research Programs at ASPI.

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