

Sounding the alarm

Terrorism threat communications with the Australian public

86

A S P I

AUSTRALIAN
STRATEGIC
POLICY
INSTITUTE

Anthony Bergin and Clare Murphy

Executive summary

A recent government review of Australia's counterterrorism machinery found that our terrorism-related metrics, including numbers of known foreign fighters, sympathisers, supporters and serious investigations, are worsening.

Our (usually classified) terrorism threat level and (public) alert level were both raised to 'high' in September 2014. This was the first time that the Australian Security Intelligence Organisation (ASIO) made the threat level public and raised it to high: we'd been on medium level for 13 years.

There was some confusion about how the public was supposed to react to the raised alert level, and about the role that terrorism advisories play in our counterterrorism machinery.



Public awareness campaign advertisements at Melbourne railway stations, October 2014 © Luis Ascui/Fairfax Syndication.

Communicating terrorism alert level warnings is a tough challenge. It's no easy task for our political leaders to find language that conveys the need to be alert, while also creating a sense of calm. But right now the public feels underinformed when it comes to terrorism advisories.

Five immediate changes could help.

- **Have one public system**

There's confusion between the terrorism threat level (which is classified by ASIO) and the public alert system. It would be sensible to collapse the two systems into one public alert system, decided by the Director-General of ASIO, that can be made public and accompanied by an unclassified narrative. ASIO's Director-General would be the national 'barometer' on terrorism alerts; he'd call the shots.

- **Introduce a sunset clause**

Lowering an alert is a rare event. There should be a sunset clause that mandates the expiry of a raised level after six months unless there's evidence that it shouldn't be changed. This would reduce costs for police, critical infrastructure operators and others who are required to mobilise extra resources when the level is high.

- **Provide geographical guidance**

A generic alert level system isn't appropriate to a country as large as the Australian continent. The Department of Foreign Affairs and Trade provides public information about risks in different countries where Australians might travel. That approach could be adapted for our terrorism warning system by making it more geographically discerning. This would strengthen the system as an effective tool for communicating useful information to the public. It would also help to tap information from the community to prevent terrorist attacks.

- **Test the narratives**

The language used for terrorism advisories shouldn't be arbitrary or ambiguous. It would be prudent to test the narratives, and especially what the system suggests that people do, at each level to see how useful the public finds them. There may well be regional or ethnic variations in how people perceive risk.

- **Launch a public awareness campaign**

A public awareness campaign communicating any changes to our terrorism advisories would be helpful. This should include social media. The Australian Government should have a national security Facebook page and Twitter account to provide information on terrorism warnings.

Introduction

Australia's terrorist threat environment is now more dangerous. Terrorism investigations are increasing in volume and complexity. A recent [Australian Government review of our counterterrorism arrangements](#) found that 'all of the terrorism-related metrics are worsening: known numbers of foreign fighters, sympathisers and supporters, serious investigations. We are not "winning" on any front.'

That sober judgement requires our counterterrorism architecture, including our primary public terrorism alert system, to be as effective as possible.

Successive Australian governments have been reluctant to change our public terrorism alert level in the absence of specific threat intelligence. The Bali bombings, the Madrid train attacks, the Australian embassy bombing in Jakarta and the London bombings didn't trigger any change to the national alert level.

But on 12 September 2014, the terrorism advisory was raised by Prime Minister Abbott from medium to high on the advice of outgoing ASIO Director-General David Irvine. Since 12 September 2001, we'd been stuck on a medium level alert; it had become, to some extent, background noise.

In our political system, the Australian Government doesn't have authority to coerce the states or business into a particular response if the alert level's raised. Successive governments have shown no appetite for dictating the states' and territories' response to terrorism advisories.

Instead, the Australian Government must convince the jurisdictions about what protective measures are needed, either by giving them fairly detailed threat information or by working with them to ensure that there's enough confidence in the overall alert system for all stakeholders to take the necessary action.

While it's not clear how much terrorist threat information the Australian Government provides to the jurisdictions and industry, it's fair to say that the general community doesn't get much actionable information from our public terrorism advisories.

Communicating danger

The Australian Government communicates with the public in many ways about terrorism threats, but does our formal public alert system make a significant contribution to our counterterrorism measures? Does it generate confidence in the public, the jurisdictions, local government and industry to take what might prove to be costly protective measures?

Public national terrorism alerts aren't a precise science. A low alert isn't a guarantee that a terrorist attack won't happen, just as a high alert is no guarantee that an attack will occur.

Absolute security from terrorism via a public warning system will remain a pipedream. Unlike a fire or flood warning that calls upon the public to take very specific actions, a terrorism advisory warning is much more general.

No terrorism advisory system can deliver perfect security or tell us exactly what we should look for—intelligence is almost never that precise. We'll need to be vigilant all the time, regardless of the alert level in force. And, unfortunately, we'll rarely know whether the alert system works: it's hard to know when a planned attack is aborted due to better security.

Overseas publics have seen alert levels raised at various times, most recently in August 2014, when the UK raised its threat level to 'severe', the second highest level.

At the same time, we've seen the rise of 'lone wolf' terrorist attacks, in which the actor merely needs intent and readily available tools, such as a car or a knife. Recent examples include the murder of drummer Lee Rigby in the UK, the attack on police officers in Melbourne, the Quebec vehicle attack, the Canadian Parliament shooting and the Martin Place siege in Sydney.

There's almost no way to predict an attack by someone who hasn't divulged his violent intentions to others and who, as a 'cleanskin', might not be known to law enforcement or intelligence agencies.

There's little doubt that lone-actor attacks have raised public doubts about the overall utility of an all-purpose general public terrorism advisory system.

However, despite the limitations of such systems, they can psychologically prepare the public by giving people an assessment of the threat at a particular time and by increasing the number of eyes and ears helping our security and law enforcement agencies.

In this sense, an alert system isn't so much about whether the intelligence community believes that something's going to happen; it's about reminding people, businesses and critical infrastructure operators to be vigilant, report suspicious activity and tailor their operations to the threat.

However, there's a paradox here. If an alert helps to deter, divert or at least defer an attack, that may reduce the public's trust in the system the next time the government wants to elevate the alert level.

Any alert system—bushfire, cyclone, terrorist attack—can contribute to the management of consequences. However, the chances of a natural hazard occurring aren't affected by the alert, and that doesn't apply to terrorism: terrorism alerts are also designed to deter attacks by making their success less certain.

The key question is whether our public national alert system helps to inform state and territory governments, businesses and citizens about what to do when conditions change.

Does a change in the level of threat tell us whether a threat is serious enough to divert time, money and people from our normal activities? And will it help us to know what to do to increase security?

Recent developments

Australia has two terrorism information systems: a national alert level that's public and a threat level that's usually classified. The threat level reflects the current assessed threat of terrorism to Australia; the alert level is intended to advise the public about the severity of the terrorist threat and how citizens should prepare.

The [National Terrorism Public Alert System](#) was first introduced in 1978 and amended to its current form in June 2003, when the highest level was introduced. It now has four levels:

- Low—terrorist attack is not expected
- Medium—terrorist attack could occur
- High—terrorist attack is likely
- Extreme—terrorist attack is imminent or has occurred.

The threat level is determined by the Director-General of ASIO. It reflects the current assessed threat of terrorism to Australia and our interests.

On 11 September 2014, ASIO raised its classified threat level from 'medium' to 'high'. The next day, the public alert level was [raised from 'medium' to 'high'](#) on the advice of the outgoing ASIO Director-General, David Irvine. The [change was announced](#) by Prime Minister Tony Abbott, David Irvine and Australian Federal Police Commissioner Andrew Colvin to a media conference in Melbourne.

It was the first time that the alert level had been raised to 'high' since the introduction of the new system; it was also the first change in 13 years, and the first time that ASIO's classified threat level was publicly disclosed.

However, it wasn't a complete surprise. Irvine had commented on 9 September that he was seriously considering raising the threat level because an estimated 20 Australians had returned from fighting in Syria and Iraq.

There had also been media speculation about raising the level here after the UK announced that it was raising its level from 'substantial' to 'severe' in August. Some Australian security experts had [urged the Abbott government](#) to follow the British lead and raise our alert level. Irvine [cited concerns](#) about people in Australia being influenced to carry out extremist violence, here or overseas.

Attorney-General George Brandis [echoed those comments](#) the next day, warning that raising the alert level was a distinct possibility. He said that this wouldn't be a political decision, but one based on the advice of our intelligence agencies.

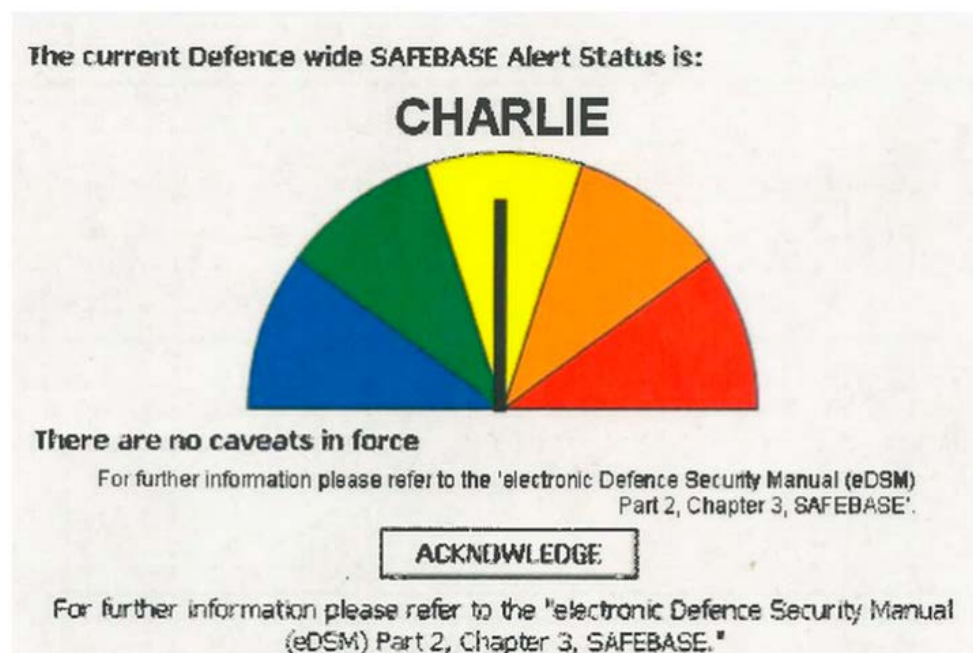
Irvine [pointed out](#) that the decision to raise the threat level was taken independently of any decisions that the government might make in relation to military interventions in the Middle East.

The Prime Minister underscored Brandis's comments that the decision to move the public alert level to 'high' was based on advice from security and intelligence agencies, rather than being a political one. (While the Prime Minister is under no obligation to accept or act on the recommendation of ASIO, it would be politically risky for him not to do so.)

Victorian Police Commissioner Ken Lay made [similar remarks](#) on the same day, agreeing that the return of foreign fighters to Australia meant that it was a suitable time to review the alert level.

Attorney-General Brandis [stated](#) that the public would notice a higher security and police presence at public events, such as the upcoming Australian rules and rugby league finals matches, but that people shouldn't be deterred from attending.

The ramifications of the heightened alert for ADF and law enforcement personnel were evident. Some military personnel were advised to [wear civilian clothing](#), instead of uniforms, when off base to protect their own security and that of their families. That advice came after security levels at Defence facilities were lifted from 'safe base Bravo' to 'safe base Charlie' for the first time since 9/11.



The SAFEbase alert level across Defence has been raised to CHARLIE.

Paramedics, firefighters and customs officers received [similar advice](#) in early October from Victorian Police Commissioner Lay. He cited the need to be alert to the changing environment as a reason for extra caution.

In January this year, the Australian Federal Police announced that its designated terror alert level was being [raised to high](#) following jihadist attacks on police and soldiers in Canada and France. The move brought the federal police into line with the public terrorism alert level. NSW police were [warned](#) to exercise discretion in their use of social media and to log into mobile data terminals whenever they got into or out of their police vehicles as an enhanced safety measure.

The Queensland Police Commissioner pointed out that there was no specific threat to his state, but he wrote to police officers and their families to remind them to ensure their personal safety. The acting Chief Commissioner of Victoria Police [outlined a range of instructions and advice](#) to his officers designed to ensure that police security was optimised.

The public might have been forgiven for being confused by the January announcement to upgrade the alert level for law enforcement: it occurred several months after the changes in the terrorism alert level for ADF bases and personnel, and was well after the Melbourne attack by Numan Haider in September 2014. Haider was shot after stabbing two Joint Counter Terrorism Team police officers.

Issues in the Australian system

Despite assurances that the decision to raise the terrorism alert level wasn't dictated by politics, several commentators suggested that the announcement was yet another example of security theatre—that the government was [‘crying wolf’](#) with vague warnings.

If no attack was imminent (and Prime Minister Abbott said none was), then why bother to make the announcement, other than to try to push through tougher security laws, such as those then before the Senate.

Others pointed out that while the public was being told not to panic, recent counterterrorism raids in Sydney, Melbourne and Brisbane [suggested some lack of transparency](#) in the reasons given for the announcement.

Senior Fairfax correspondent [Daniel Flitton](#) judged that the public were no better informed or protected as a result of raising the rating to high. The only consequence was an ‘initial burst of panic and unfair suspicion . . . when nothing happens, or is seen to have happened, complacency will set in’.

There was some very understandable media confusion about the language used in announcements about the threat level and the public alert. Even though the threat level is determined by a classified system while the alert level is public, media commentary didn't distinguish the two at the time of the announcement.

When Abbott, Irvine and Colvin instructed the Australian people to go about their daily activities and not allow the elevated alert level to influence their behaviour, some asked whether the language used in raising the alert from medium (an attack ‘could’ occur) to high (an attack was ‘likely’), was precise enough to help the public understand what they should do in response.

Another question wasn't raised at the time: does a public national alert system that sets out the general level of threat make much sense in a country the size of Australia? A threat to a Sydney shopping mall might not necessitate taking workers off Western Australian offshore installations.

It's true that most Australian state and territory police or first ministers' departments make some reference to the terrorism alert level on their websites, and that some refer to counterterrorism efforts being made in their jurisdictions. But they normally just refer the public back to the Australian Government's [national security website](#) (Table 1).

Table 1: Jurisdictional public information on terrorism advisories

State/territory	Government	Police
New South Wales	SecureNSW , the NSW government's official counterterrorism website, states and summarises the current level, summarises the NSW security environment, and refers the public to the National Security Hotline and ASIO.	Summarises the Commissioner's speech announcing the rise in level to 'high', answers FAQs, summarises the NSW Police groups responsible for counterterrorism arrangements and provides a link to the NSW counter terrorism plan. It directs people to the National Security Hotline and the national website.
Victoria	No reference to the terror alert.	Summarises the National Terrorism Public Alert System, its purpose and how it affects the public, and directs people to the national website.
Queensland	Safeguarding Queensland , the central source of counterterrorism information, states the alert level, refers the public to the National Security hotline and provides information on the Security and Counter-Terrorism Group, which is part of Queensland Police. The Queensland Government website outlines the alert levels, advises on public behaviour and outlines the Queensland Government and Queensland Police role in countering terrorism.	Outlines the purpose and details of the Intelligence and Counter-Terrorism Major Command and the Security and Counter-Terrorism Group.
Western Australia	The Department of the Premier and Cabinet website summarises the current alert level, advises on behaviour and directs the public to the national website. It refers to the role of the Office of State Security and Emergency Coordination within the department in supporting Western Australia's involvement in national counterterrorism arrangements in collaboration with WA Police and in advising and supporting the Premier.	Summarises the National Terrorism Public Alert System, its purpose and how it affects the public, and directs people to the national website. States that the Prime Minister will inform the public of a change in the alert level, and that the Western Australian Premier will provide further information in the event of an incident specific to Western Australia.
South Australia	No specific reference to a national or state terror threat level on the websites of the Department of the Premier and Cabinet or the South Australian Government.	Summarises the current alert and how it affects the public and directs people to SA Police resources and the national website. Refers to community engagement and SA Police's work with other police and national security agencies to counter terrorism.
Tasmania	TasALERT , the official emergency information source, summarises the National Terror Public Alert System, states the alert level, advises on behaviour and directs people to the national website. It states that Tasmanian Police will inform and guide TasALERT in the event of a terrorist incident, and that the Special Response and Counter-Terrorism Unit leads Tasmanian Government activities to prevent, respond to and recover from terrorist threats.	Refers to separate policing threat level and directs people to the national website. States that the Special Response and Counter-Terrorism Unit is the focal point for Tasmanian Government counterterrorism activities, and establishes the arrangements for prevention, response and recovery in relation to terrorist threats.

State/territory	Government	Police
Northern Territory	<p>SecureNT, the official emergency information source, directs people to the national website.</p> <p>The website of the Department of the Chief Minister states the alert level, and that the department works closely with the NT Police Security and Emergency Section and with other territory organisations with roles in responding to the consequences of a terrorist act. It states that changes to the threat level that affect the territory will be communicated by both the Prime Minister and the territory's Chief Minister, and directs the public to the national website.</p>	No reference to the National Terrorism Public Alert System.
Australian Capital Territory	No reference to the National Terrorism Public Alert System.	No reference to the National Terrorism Public Alert System.

Natural hazards warnings are currently pushed to members of the public via Web 2.0 services, but it isn't clear that people would know where to look to find terrorism advisories in their home state or territory. In the case of the Australian Capital Territory, there's no reference to the terrorism alert level on the territory's government websites. A number of jurisdictions note that the premier, the chief minister or the police will provide additional information to the public in the event of a terrorist attack.

International comparisons

The **United Kingdom** public terrorism alert system is a tiered system, like ours, but with slight differences in language and an extra level:

- Low—an attack is unlikely
- Moderate—an attack is possible, but not likely
- Substantial—an attack is a strong possibility
- Severe—an attack is highly likely
- Critical—an attack is expected imminently.

Assessments of the level and nature of the threat are made by the Joint Terrorism Analysis Centre. The Security Service is responsible for setting the threat levels from Irish and other domestic terrorism in Northern Ireland and Great Britain. The system distinguishes different alert levels for terrorism related to Northern Ireland and for international terrorism.

The **United States** Department of Homeland Security introduced the Security Advisory System in 2002, in the wake of the 9/11 attacks. In 2011, the National Terrorism Advisory System (NTAS) replaced the colour-coded advisory system. The change was intended to more effectively communicate information about terrorist threats by providing timely, detailed information to the public, government agencies, first responders, airports and other transportation hubs, and the private sector.

The system includes both imminent and elevated threat warnings. An imminent threat signals a credible, specific and impending terrorist threat against the US, whereas an elevated threat warns of a credible terrorist threat. In collaboration with other federal entities, the Department of Homeland Security decides which NTAS alert will be issued and when. Alerts are only to be issued for finite—and generally short—periods.

NTAS alerts are distributed via the department's official NTAS webpage, email alerts, data feeds and social media. Alerts are shared in public and private spaces, such as transit hubs and government buildings.

Surprisingly, no unclassified NTAS alert has ever been issued, even after such events as the killing of bin Laden (there were fears of revenge attacks), the tenth anniversary of the 9/11 attacks (there were credible fears of an attack in New York or Washington), and the Boston Marathon bombing.

However, the US has a network of public-private partnerships grouped by critical infrastructure areas connected by the Department of Homeland Security, and in a parallel system of special interest groups sponsored by FBI field offices. For example, the banks and financial institutions in major cities meet informally under FBI sponsorship and share threat information.

With the two parallel systems, specific alerts can be passed to the people who need them most (say, people working in critical infrastructure), without making public announcements. The department and the FBI use a parallel law enforcement organisation system to pass alerts through 'fusion centers' and joint terrorism task forces.

France has a national terrorism alert system, *Plan Vigipirate*, that's been upgraded a number of times since 1995 to become a colour-coded model.

In February 2014, the levels were simplified to 'vigilance' and 'attack alert'. France is permanently on vigilance alert level. It switches to *alerte attentat* level when the threat is considered to be imminent.

Vigilance means a permanent security posture: control and screening measures; surveillance in public transport and inspection in some trains; surveillance in heavily frequented places; and access control in government buildings. This level can be slightly upgraded in a specific place for a limited time, but the public isn't automatically informed of it.

Alerte attentat points to an increase in the terrorist threat. This alert level means that France can take exceptional measures when it faces an imminent threat of a terror attack (either if the terror attack has happened, such as the Charlie Hebdo and Jewish shop attacks in January 2015, or if the risk is very high). The alert can be implemented in a limited zone or over the whole territory, and is limited to a short period.

Specific measures that can be taken include deploying response capabilities (law enforcement and emergency or rescue services); banning parking around schools; strengthening controls over explosives; activating crisis units in ministries and prefectures and sensitive infrastructure; and reinforcing the armed forces' contribution to surveillance.

The public is informed about the evolution of the terror threat and on the change of Vigipirate posture by declarations from the Prime Minister or other relevant ministers, and through the government's [risk website](#), which provides updated information on the situation and the Vigipirate plan.

The model can be likened to an electricity switch that's turned on at times when danger is perceived to be heightened. It maintains public and police vigilance by maintaining a high alert only when absolutely necessary.

Spain uses a three-level response plan called the Terrorism Prevention and Protection Plan, the highest level of which requires increased screening of passengers on public transport and heightened security around critical infrastructure.

The level was [most recently raised](#) following the Charlie Hebdo attacks in Paris, from 'high-intensity two' to 'low-intensity three'. This resulted in an increase in surveillance and protection of areas that would possibly be targeted by terrorists, such as airports, train stations and centres of critical infrastructure.

New Zealand employs a six-tier terrorism alert system. The threat level is determined and issued by the [Combined Threat Assessment Group](#), which comprises the police, the New Zealand Security Intelligence Service, the New Zealand Defence Force and the Government Communications Security Bureau.

The New Zealand system is barely used. Prime Minister Key's [announcement](#) that the level had gone up from 'very low' to 'low' last October was the first public confirmation of the alert level in New Zealand's history.

Israel's alert system consists of four alert levels (1 is the lowest and 4 is the highest). It's a relatively informal system and doesn't have much public impact—there's no formal national alert system. This approach makes sense in Israel's context: the terrorist threat level would almost always be at 'imminent', with a terrorist attack assessed as likely. There isn't the same need for public education and awareness in Israel as in many Western countries; the Israeli public has a high degree of awareness of terrorism threats.

Alerts tend to be in response to specific threats. They're time and area demarcated, and usually issued through the police or Israel Defense Forces spokespeople. Various news notification services then pass them on, but there's nothing more formal than that.

Alerts are issued when the police (informed by the intelligence agencies) believe there's a specific need when they have information about a possible attack, but the alert is more for police operational purposes.

The Israel Defense Forces have their own terrorism alert system, which isn't public. For Israeli citizens, the system is somewhat ad hoc; for example, they'll receive alerts about roads being blocked because of policing activities or an expected protest. Police categorise zones with numbers on the level of danger. The Counter Terrorism Bureau issues travel warnings for Israelis on an ad hoc basis, informed by particular events or intelligence.

Canada has never had a public terrorism threat alert system. However, it has a threat level system that operates as an internal tool for security agencies to inform potential first responders of the current threat level in the country.

Last year, Canada raised that threat level from 'low' to 'medium'. Canadian authorities stated that this meant that intelligence indicated that an individual or group within Canada or abroad had the intent and capability to commit an act of terrorism. The [level was raised](#) just two days before a series of shootings in Ottawa.

Germany also lacks formal public terrorism alert systems at either the federal or the state level, but there's recently been heightened security around specific places of possible terrorist interest.

Counter-terrorism machinery review

The most recent discussion of our national terrorism alert system is set out in the Australian Government's [Review of Australia's counter-terrorism machinery](#), which was released in January 2015.

The key findings of the review, as it related to national terrorism advisories, were as follows:

- The current system, with separate classified and public levels, is unnecessarily complex, both for the public and for officials.
- There aren't enough public levels, making it difficult to raise or lower the alert level in response to a temporarily increased threat environment.
- With more media attention, there's a public expectation that the government will provide useful information on terrorist threats and advice about required changes to behaviour.

The review proposed that the threat level be made public by the Director-General of ASIO and accompanied by an unclassified narrative. The public alert system would no longer be required, so there'd be only one system in place.

There'd be some minor changes to threat level descriptions, but ASIO's threat assessments and all supporting intelligence would remain classified. In deciding to raise the threat level, ASIO would continue to consult with the jurisdictions.

As a result of the review's finding that there isn't enough flexibility or precision in the definition of the levels, it recommended a new model (see figures 1 and 2).

Figure 1: Current and proposed threat levels

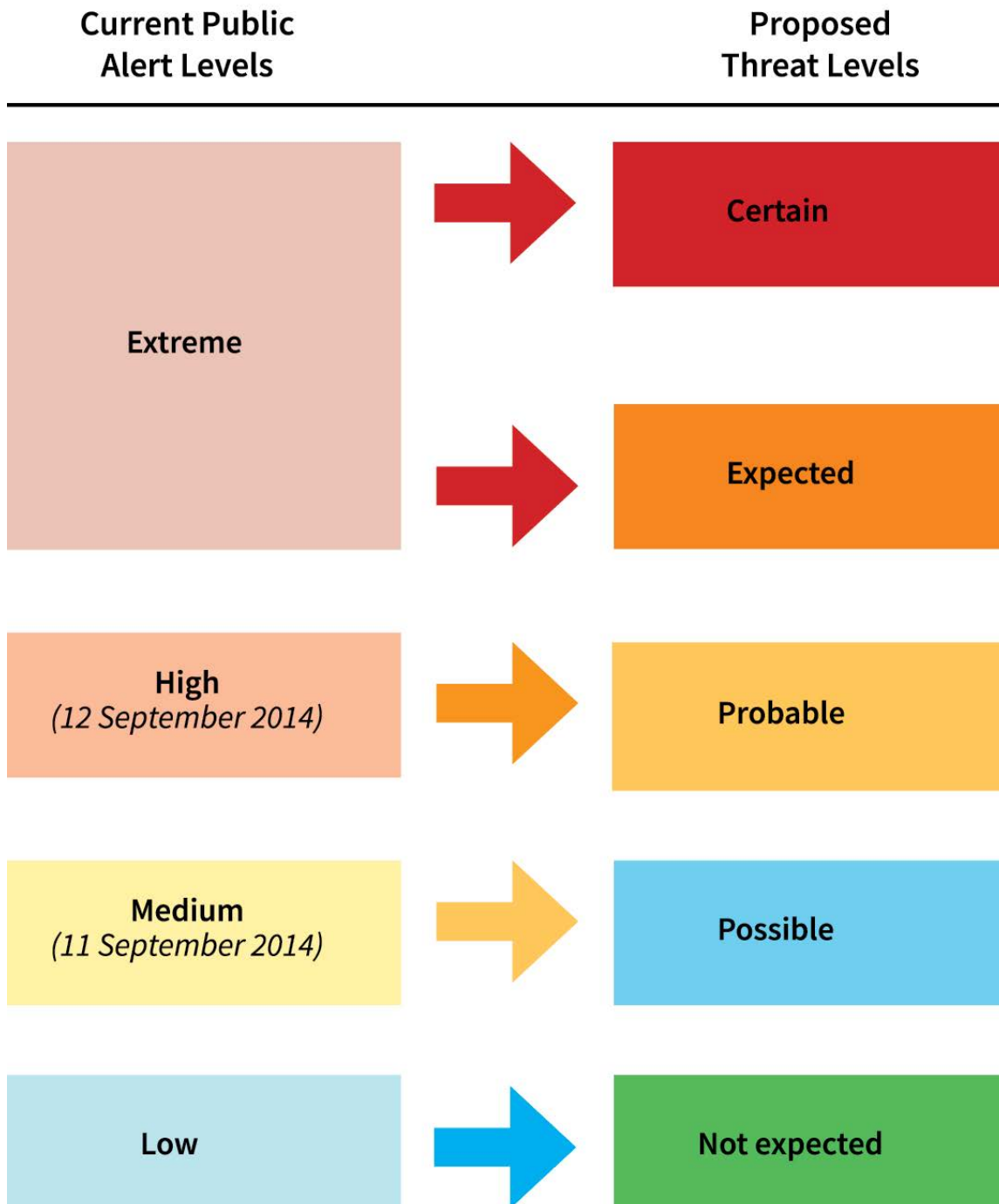
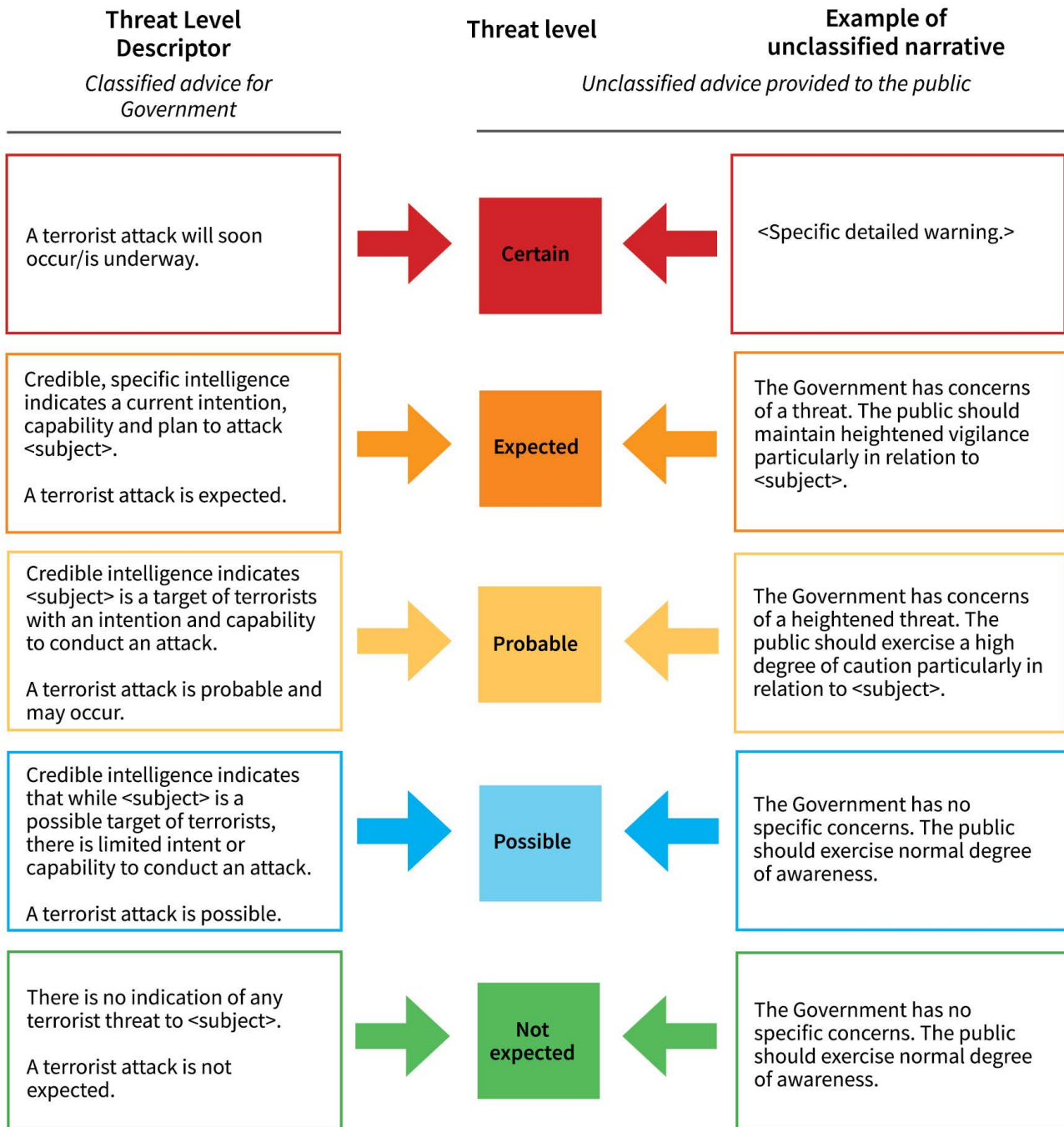


Figure 2: New model descriptors and example advisories



Source: *Review of Australia's counter-terrorism machinery*, Chart 14, page 45.

The new model replaces levels (low, medium, high, extreme) with terms describing the likelihood of a terrorist attack occurring (not expected, possible, probable, expected, certain). It has five levels, one more than the current advisory system.

Later this year, the review's suggestions will be put to the Australia – New Zealand Counter-Terrorism Committee for consideration.

Five recommendations to strengthen our terrorism advisories

Any terrorism advisory system will have limitations: intelligence usually doesn't supply precise details to establish exactly when an attack might happen, and there are often problems in notifying the public about a threat that isn't well defined.

However, we're better off having a formal system that offers consistent information to the public and helps in preventing and surviving terrorism, while also guiding the activities of business and infrastructure operators, than having no system at all.

Have one public system

The recent review of Australia's counterterrorism machinery correctly found that there's confusion between the threat and alerts systems.

It would be sensible to collapse the two systems into one public alert system that's decided by the Director-General (DG) of ASIO and that can be made public and accompanied by an unclassified narrative. The DG would be the national terrorism 'barometer' on terrorism alerts and would call the shots.

This would eliminate confusion over both the Prime Minister and the DG announcing threat levels. It would help to depoliticise the issuing of threat warnings by removing the Prime Minister from the process and would promote greater public confidence in our overall counterterrorism arrangements.

The change would be consistent with the functions of the DG, as set out in the ASIO Act. The Act doesn't empower the minister to override the DG's opinion about the nature of ASIO's advice, and requires the DG to take all reasonable steps to ensure that ASIO's 'kept free from any influences or considerations not relevant to its functions'. It also requires that nothing should be done that might lend colour to any suggestion that ASIO is 'concerned to further or protect the interests of any particular section of the community, or with any matters other than the discharge of its functions'.

Introduce a sunset clause

While rises in terrorism threat levels are common, there have been few cases of alert levels being lowered. There's an inherent difficulty in lowering a terror alert: unlike weather or fire alerts, terror alerts aren't backed by scientific data indicating that a threat has reached its peak and declined.

Lowering an alert may run the risk of lulling law enforcement agencies and the public into a false sense of security: terrorists may choose to attack during a time of a lowered alert, when our guard's down.

A sunset clause—the mandatory expiration of a raised level after six months—would allow the level to be lowered objectively. It would provide enough time for intelligence and law enforcement agencies to assess the situation. This would reduce the risk that an elevated level just becomes the 'new normal'. There's some community expectation that at some point the level could go down. For example, there may arguably have been times in the 13 years after 9/11 when we might have lowered the alert level from 'medium'.

There'd be some risk that scaling alerts up and down could diminish public confidence if there were regular shifts. However, we're unlikely to see the earlier US pattern after 9/11 of quickly raising and lowering alert levels, which attracted derision. There were perceptions that the US colour-coded system was being manipulated for political purposes.

The mandatory lowering of an alert after a certain period, unless there's evidence that it shouldn't be changed, would reduce the costs associated with remaining at elevated alert levels, such as the costs of critical infrastructure operators and police.

Provide geographical guidance

The Australian jurisdictions don't have a consistent approach to communicating risk to their communities through the current terrorism alert system.

However, a generic national alert level system isn't appropriate for a country as large as Australia. Even the state or territory level might not be appropriate: Victoria used to issue fire warnings for the whole state, but that system's now been replaced with more precise geographical information.

The Department of Foreign Affairs and Trade provides [public information on risks](#) in different countries where Australians might travel, and the public is familiar with that system.

Such an approach might be adapted to make our terrorism warning system more geographically discerning. Other large countries, such as the US, have alert systems able to provide warnings for specific regions.

A change along these lines would strengthen our system as an effective tool for communicating useful information to the public. It would also help to tap information from the public to prevent terrorist attacks.

Measured information could be set out in the narrative for the declared alert level. While some state governments and the tourism sector might not welcome the highlighting of a particular region, the public already understands that the risk of a security incident is higher in some places than others. Such a change would give the public greater confidence in terrorism advisories.

Providing more geographically targeted information is unlikely to cause unnecessary concern or panic in the community and would promote the need for individual preparedness.

Test the narratives

The language in the current alert system is somewhat arbitrary, although it's no easy task for our political leaders and security agencies to find language that [conveys the need to be alert](#), while also avoiding ambiguity and creating a sense of calm.

Before adopting the new model proposed by the review of our counterterrorism machinery, it would be prudent to test the narratives at each level with the public to see how useful people find them, and especially what the system suggests people should do at each level.

There may well be regional and ethnic variations in how communities, parts of communities or individuals perceive risk. The NSW Premier's Department's [Behavioural Insights Unit](#) could contribute to this work.

One way to test the language would be to look at the warnings used by meteorological advisory systems. Obviously, distinctions have to be made between terrorism alerts and weather alerts. Terrorism warnings aren't nearly as scientific and rely on classified information, which must be protected, and it's much more certain when a weather threat is looming and when it has passed.

However, the public is used to acting upon natural hazard warnings, and the firefighting and weather agencies have gradually improved their warning systems. Victorian authorities changed the language of their warnings after the Black Saturday bushfires in 2009, making the highest level 'Code Red' (other jurisdictions, such as NSW and Queensland, use the term 'catastrophic'). Warnings about rain have also changed. For example, the [Bureau of Meteorology](#) has replaced terms that people found ambiguous: instead of stating that there's 'a chance of rain', the bureau now uses words such as 'possible' or 'likely'.

Launch a public awareness campaign

Victoria got onto the public communications front foot after the heightened alert in September 2014 by displaying large advertisements for the National Security website at metropolitan train stations. The Public Transport Users Association expressed its support, stating that it hoped the campaign would encourage commuters to report suspicious objects or individuals without causing panic.

A public awareness campaign communicating any changes to our terrorism advisories would be helpful. It should use the media, including social media, to educate the public about the changes. It would be useful to have an Australian Government national security Facebook page and a Twitter account to provide information on terrorism threats and warnings, encourage engagement with the community and provide resources for those with concerns. The US Department of Homeland Security [Twitter account](#) might be a useful model.

In the communications campaign, it will be important to emphasise what people should do to enhance their individual preparedness and to stress the need for vigilance and the prompt reporting of suspicious activities.

Acronyms and abbreviations

ADF	Australian Defence Force
ASIO	Australian Security Intelligence Organisation
DG	Director-General of ASIO
FBI	Federal Bureau of Investigation (US)
NSW	New South Wales
NTAS	National Terrorism Advisory System (US)

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 the authors

Anthony Bergin is Deputy Director at ASPI.

Clare Murphy is a research analyst at ASPI.

Acknowledgement

The authors thank Hayley Channer for help with information on terrorism alerts in other countries.

About Strategic Insights

Strategic Insights are shorter studies intended to provide expert perspectives on topical policy issues. They 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

Blog www.aspistrategist.org.au

 [Facebook.com/ASPI.org](https://www.facebook.com/ASPI.org)

 [@ASPI_org](https://twitter.com/ASPI_org)

© The Australian Strategic Policy Institute Limited 2015

This publication is subject to copyright. Except as permitted under the *Copyright Act 1968*, no part of it may in any form or by any means (electronic, mechanical, microcopying, photocopying, recording or otherwise) be reproduced, stored in a retrieval system or transmitted without prior written permission. Enquiries should be addressed to the publishers.

Notwithstanding the above, Educational Institutions (including Schools, Independent Colleges, Universities, and TAFEs) are granted permission to make copies of copyrighted works strictly for educational purposes without explicit permission from ASPI and free of charge.