Australian Government

Department of the
Prime Minister and Cabinet

January 2015

Review of Australia's Counter-Terrorism Machinery

ISBN 978-1-925237-36-8 (Hardcopy)
ISBN 978-1-925237-37-5 (PDF)
ISBN 978-1-925237-38-2 (DOC)

Contents

Executive Summary

Review of the Commonwealth's counter-terrorism arrangements

The Commonwealth has strong, well-coordinated counter-terrorism (CT) arrangements. Overall, these have been quite successful – although the Martin Place siege and the stabbing of police in Melbourne raise questions.

- Many plots – some quite major – have been disrupted.
- There have been 35 prosecutions and 26 convictions.
- There has been no large scale terrorist attack on Australian soil in the post-2001 period. The three fatalities within this period all happened in the Martin Place siege.

The two terrorist attacks in that period – the stabbing of two policemen in Melbourne and the Martin Place siege with its two tragic victims – were carried out by individuals who planned and acted alone. Crimes planned like this are, by nature, always extremely difficult for police and security agencies to prevent.

In the years since 11 September 2001:

- many more departments and agencies have been drawn into the CT effort. Coordination is better than ever
- new legislation has been progressively introduced to provide the legal tools to prosecute terrorists and better disrupt support to terrorism
- modest efforts to counter violent extremist ideology and to promote community cohesion are now underway.

The rising tide of terrorism

The threat of terrorism in Australia is rising and it is becoming harder to combat.

- There are an increasing number of Australians joining extremist groups overseas.
- There are an increasing number of potential terrorists, supporters and sympathisers in our community.
- There is a trend to low-tech 'lone actor' attacks which are exponentially harder to disrupt: there may be no visibility of planning and no time delay between intent and action.
- There is now an intergenerational dimension, with the families of known terrorists increasingly radicalised and involved.
- The international forces driving terrorist ideology and capabilities are stronger, and extremist narratives have increasing appeal in the Australian community.
- Terrorists are using sophisticated technologies and methodologies to stay under the radar.
- Terrorists are now adept at exploiting social media to distribute polished propaganda products.

Reflecting this environment, there is an increasing requirement for early disruption of terrorist plans to best ensure public safety. This comes at the cost of securing sufficient evidence to prosecute.

- This leaves potential terrorists at large. It also erodes trust, confidence and relationships with at-risk communities. It may also undermine public confidence in national security agencies and the Government generally.

Winning many battles – but not the war

Despite improvements in CT capability, a terrorist attack is possible. 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.

The Martin Place siege and the Melbourne attack on police are examples of a global trend: we face an increasing number of potential terrorists who are hard to detect and often willing to attack using quickly implemented, low-tech tactics.

Responding to this worsening threat picture, on 4 August 2014 the Government boosted funding to CT activities. National security agencies are significantly bolstering their capabilities to detect and disrupt the threats we face.

Every dollar must be spent wisely. We face a new paradigm that demands ever more careful prioritisation. National security agencies must come together seamlessly around shared priorities.

A restructure or reshuffle of national security agencies is not the answer. But more must be done to strengthen cross-agency coordination and leadership.

Whatever we do, there is no short-term solution to our evolving terrorist challenge. It is almost inevitable that we will have more terrorist attacks on Australian soil.

Long term, we must put a greater effort into reducing – rather than managing – the pool of terrorists, their supporters and sympathisers.

The community is key.

To counter violent extremism we must work with our at-risk communities. We must build resilience to terrorist ideology and assist individuals to disengage and de-radicalise from violent extremist beliefs and influences.

Future direction

To combat the challenge most effectively, we need to:

5. acknowledge that we have entered a new, long-term paradigm of heightened terrorism threat with a much more significant 'home grown' element
6. further improve and broaden the scope of our national CT strategy to provide a clear direction to the national security community and to improve our cooperation with at-risk communities
7. strengthen further cross-agency leadership and coordination by designating a National CT Coordinator as the Government's leading advisor on CT
8. develop a COAG strategy to counter violent extremism, increasing Australia's national commitment to this work
9. better manage increasing resource pressures by tightening priorities and lessening the burden of the efficiency dividend on some areas of national security agencies
10. improve our communication with the public on CT threats by introducing a single threat level system to improve usability and to give the public more meaningful information.

Recommendations

Leadership and coordination

1. The Government, in close consultation with states and territories through the Australia-New Zealand Counter-Terrorism Committee (ANZCTC), develop a new national counter-terrorism (CT) strategy which appropriately coordinates and balances our efforts to counteract the various threats we face, including from home-grown lone actors and radicalisation in our community.
2. The Government implement the following arrangements to provide strong, clear and co-ordinated leadership to ensure agencies respond effectively and appropriately to terrorism:
    a. designate a senior official as the National CT Coordinator.
    b. establish a Senior Executive Counter-Terrorism Group (Executive Group), chaired by the National CT Coordinator, to set the strategic direction for the Commonwealth's CT efforts.
    c. mandate that the Australian Counter-Terrorism Centre draw together policy and operational agencies, including secondees from the states and territories, to work together closely on operations, policy challenges and capability development.

Community cohesion

3. The Government significantly boost Counter Violent Extremism (CVE) activities:
    a. seek COAG agreement to a new national CVE strategy for endorsement in 2015, increasing Australia's national commitment to this work
    b. the Attorney-General bring forward a proposal as part of this effort with options to:
        i. establish and expand community and public-private partnerships to better reach at-risk or radicalised individuals
        ii. expand Commonwealth efforts to address the causes of violent extremism in Australia.
    c. the Attorney-General lead development of a strategy to counter the reach of extremist narratives in Australia.
4. The Attorney-General's Department coordinate across government to develop a strategy for managing the controlled return of Australian foreign fighters, subject to the Government's imposition of stringent, individually-tailored terms and conditions on returnees.

Resourcing pressures

5. The Government adjust its approach to seeking efficiencies from the national security agencies by:
   a. from 2015-16, removing the efficiency dividend (ED) from all of the ASIO, ASIS, and AFP operations
   b. from 2015-16, ending the application of the ED to the ONA and the OIGIS
   c. in-principle, from 2015-16, removing the ED from all ACBPS operations that will transition to the new DIBP including the Australian Border Force with final costs to be agreed with the Department of Finance and a detailed proposal brought to NSC by 30 June 2015
   d. noting that the AFP, ASIO, ASIS, DIBP and ONA would be subject to the ongoing whole-of-government non-ED efficiency processes, including the functional and efficiency reviews, including the Efficiency through Contestability Programme.

   Alternatively:

   e. from 2015-16 applying a 0.5 per cent ED to ASIO, ASIS and AFP operations, to all ONA and OIGIS funding, and in-principle applying a 0.5 per cent ED to all ACBPS operations that will transition to the new DIBP with final costs to be agreed with the Department of Finance and a detailed proposal brought to NSC by 30 June 2015.

Public advisories

6. The Attorney-General refer the modified national threat advisory system to the ANZCTC for consideration.

Part One:
THE STATE OF PLAY

One: Australia – our evolving approach to countering terrorism

Key points

The Commonwealth's CT machinery has evolved significantly in the 14 years since the 11 September 2001 attacks.

Many more agencies have been drawn into CT activities. Agencies have become better coordinated – with strong relationships across government and with external partners. Agencies have also become more capable – with improved legislative powers and greater resources.

Today, our national efforts are focussed on:

- *disrupting attacks*
- *undermining terrorist activities and support*
- *promoting community cohesion.*

States and territories play an equally important role in these efforts, and the Commonwealth's efforts must complement state and territory actions.

On 4 August 2014, the National Security Committee of Cabinet (NSC) agreed that the Department of the Prime Minister and Cabinet would lead a review of Australia's CT arrangements, to ensure they are as well-organised, targeted and effective as possible.

In fulfilling its mandate, the Review interviewed officials from agencies across the CT community, including agency heads and secretaries and state and territory officials; examined principles and findings from previous reviews; considered international comparisons; analysed the history of current arrangements; and considered the implications of the changed threat environment.

While the Review is focussed solely on Commonwealth activity, Australia's national approach to countering terrorism means that many of our efforts depend on collaboration with state and territory governments.

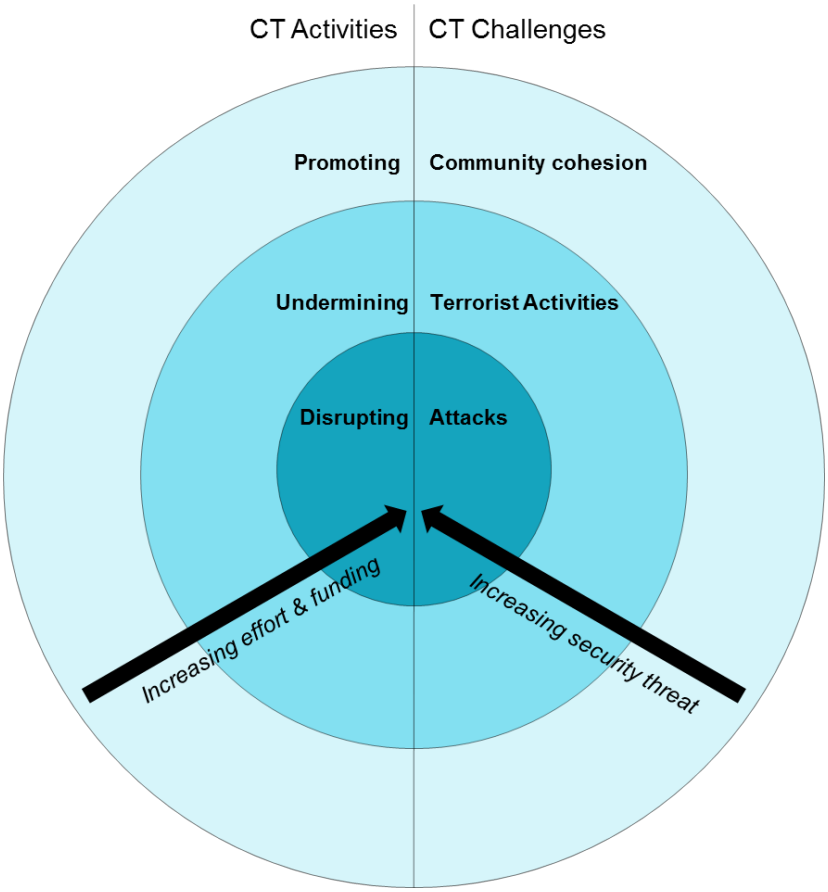
This Review does not cover the lessons learnt from the Martin Place siege, which is subject to a separate review announced on 17 December 2014 and a New South Wales Coronial Inquiry.

The activities of our CT machinery

To effectively counter terrorism, Australian governments must work across a spectrum of activity, as represented in Chart 1, to:

1. **disrupt** the activities of individuals or groups planning an attack
2. detect and **undermine** terrorist activity by:
   a. blocking the flow of support (finances, goods and people) to or from terrorists and their networks
   b. impeding the development of terrorist capability (particularly their tactical and operational security training both directly and online)
   c. degrading ideological support for terrorist activities.
3. **promote** community cohesion and build resilience to radicalisation.

Chart 1: The spectrum of CT efforts



The development of Australia's CT framework – events and responses

The terrorist attacks in the United States on 11 September 2001 were a major turning point in Western understanding of the threat from Islamist terrorism.

Governments across the world responded by significantly boosting their CT capabilities. In Australia, from 2001-02 to 2013-14, the overall budget of the Australian Security Intelligence Organisation (ASIO) was increased more than fivefold; that of the Office of National Assessments (ONA) almost quadrupled; for the Australian Secret Intelligence Service (ASIS) it more than tripled and for the Australian Federal Police (AFP) it more than doubled.

New legislation was introduced to criminalise terrorist acts and the provision of support for terrorism. Other new legislation provided additional powers to national security agencies. This new legislation included revisions to control orders which better enabled the AFP to place restrictions on an individual in order to protect the public from a terrorist act.

As both the number of national security agencies responding to the CT challenge and the complexity of the CT challenge itself grew, governance and coordination structures were enhanced to avoid 'siloing'. The emphasis was on information sharing and cooperation, both domestically and internationally. Agencies became better coordinated with strong relationships across government. They also became more capable – with improved legislative powers and greater resources. The age-old intelligence community mantra on information sharing 'need to know' was replaced with a new motto 'need to share'.

Today, we face new terrorist threats and renewed scrutiny of our CT capabilities and coordination. This section describes the evolution of the Commonwealth's CT machinery from 2001 to 2014.

Understanding how we arrived at this point helps answer the question – where to from here?

Chart 2 – Significant terrorism events and Australian CT response : 2001 – 2014

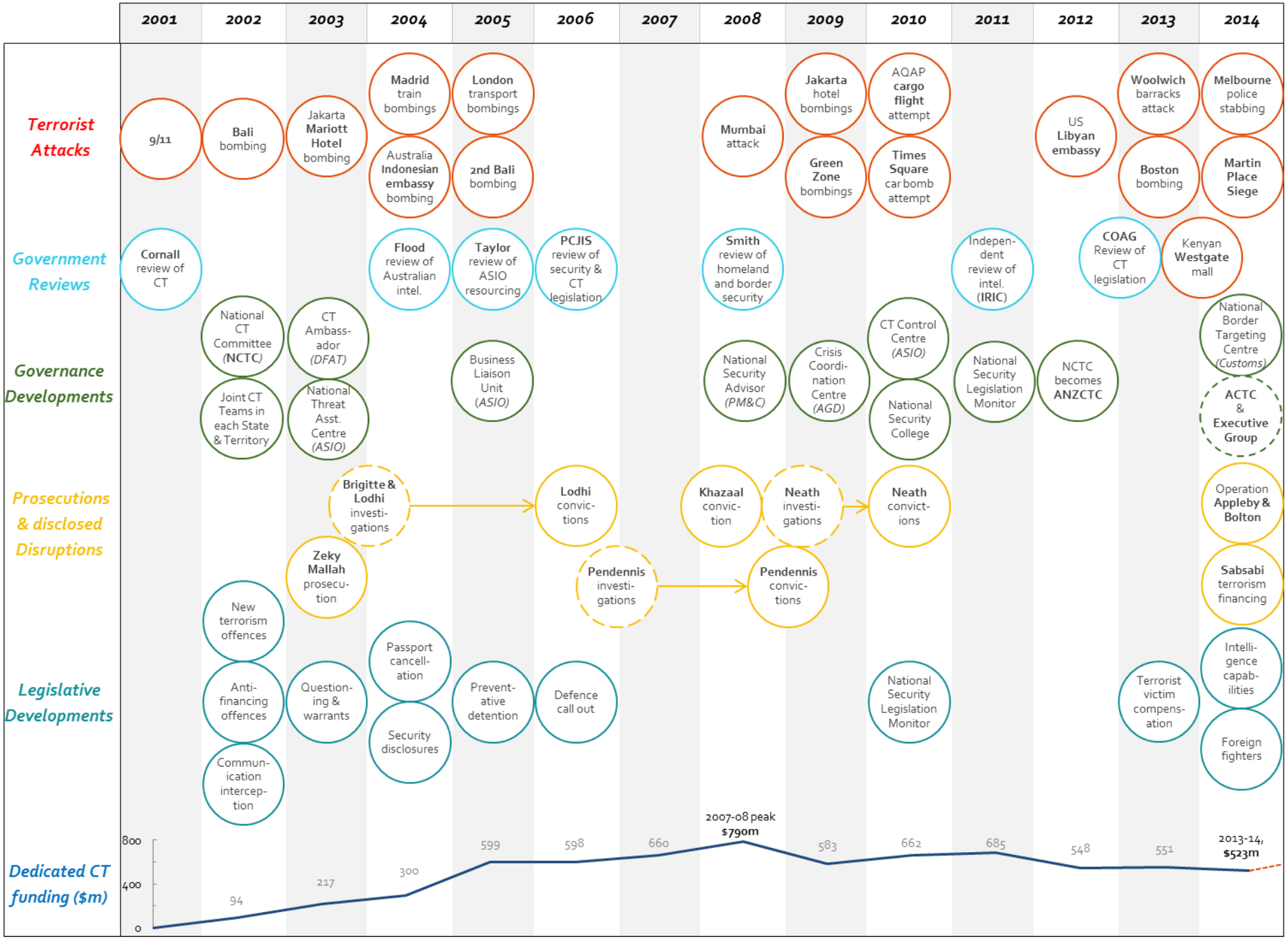
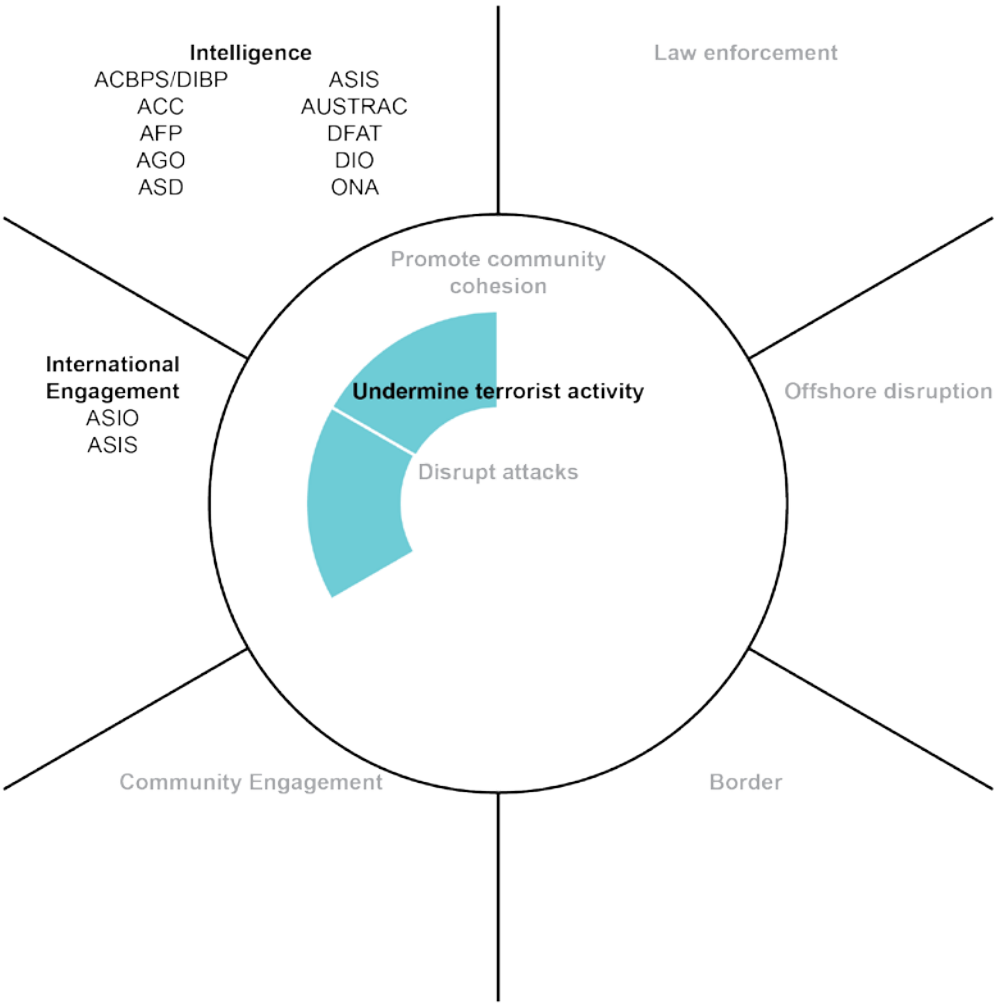


Chart 3: Commonwealth CT functions and activities prior to 2001



Prior to 2001 there were few agencies involved in CT activities and even these were only involved in undermining terrorist activity. The number of agencies, and this pattern of involvement, was to change sharply over the following decade. (Note Chart 5 on page 11.)

2001 – 2003

The events of 11 September 2001, the 2002 Bali bombings and the 2003 Jakarta Marriot bombing put terrorism at the forefront of public concerns in Australia. This prioritised CT within the Australian intelligence community and increased the number of agencies responding to the terrorism threat.

- In 2002, in response to the recommendations of the 2001 Cornall Review, the Government introduced new legislation defining a range of specific terrorism-related offences and enabling the proscription of terrorist organisations.
- In 2003, Sydney-based Australian citizen Zaky Mallah was the first person charged under the new terrorism legislation.

Governance changes in 2002 and 2003 included:

- the establishment of the National Counter-Terrorism Committee (NCTC) as a focal point for national CT policy and capability development
- the formation of the National Threat Assessment Centre (NTAC) within ASIO to issue threat assessments. NTAC includes representatives from eight Commonwealth agencies and one state agency

- the establishment of the Trusted Information Sharing Network for Critical Infrastructure Resilience. This provides an opportunity for government to share vital information to protect Australia's critical infrastructure and the continuity of essential services
- the appointment of a Counter-Terrorism Ambassador within DFAT to lead and coordinate collaboration between Australian agencies and international partners.

In 2002, Joint-Counter Terrorism Teams (JCTTs) were established comprising representatives from the AFP, state and territory police forces, ASIO and other agencies.

Australian participation in CT investigations offshore, such as the 2003 investigations into the Bali bombing, provided opportunities to assist in CT capacity building and policy development with a wide range of partners.

2004 – 2007

There were several major overseas terrorist attacks during this period. In Australia, there were further prosecutions under the terrorism legislation. Governance arrangements were stable but CT legislation continued to be strengthened.

The Madrid and London transport bombings highlighted new avenues of attack against 'softer' civilian infrastructure targets in major Western capitals. A second Bali bombing and the bombing of the Australian embassy in Jakarta reinforced regional concerns.

In response to the 2004 Flood Review into Australian Intelligence, agencies improved coordination on CT and addressed gaps in the collection of intelligence on regional terrorists. For example, ASIO established a unit comprising representatives from Australian intelligence agencies to assess and inform collection of the activities and associations of regional terrorists.[1]

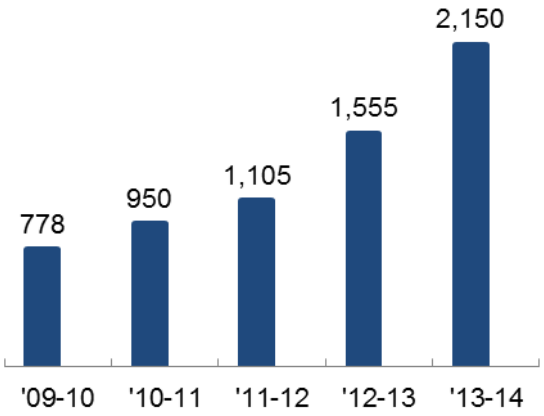
In 2004 the Business-Government Advisory Group on National Security was established to provide a mechanism for the Australian Government to discuss a broad range of national security issues and initiatives with CEOs and senior business leaders. This has been reinvigorated in 2014 as the Attorney-General's Industry Consultation on National Security.

The 2005 Taylor Review of ASIO's resourcing found the number of priority CT investigations had quadrupled. It found ASIO's priority setting, risk management approach and performance monitoring processes were thorough.

Further legislation was introduced, including new ASIO powers to coercively question persons under warrant in relation to terrorism offences and AFP powers to seek preventative detention orders to prevent an imminent terrorist attack and/or the loss of vital information immediately after a terrorist act.

The Business Liaison Unit (BLU) was established in 2005 to ensure that owners and operators of critical infrastructure and other relevant members of the Australian business community could access timely ASIO information on matters affecting the security of their staff and assets.

Chart 4: Number of ASIO BLU subscribers

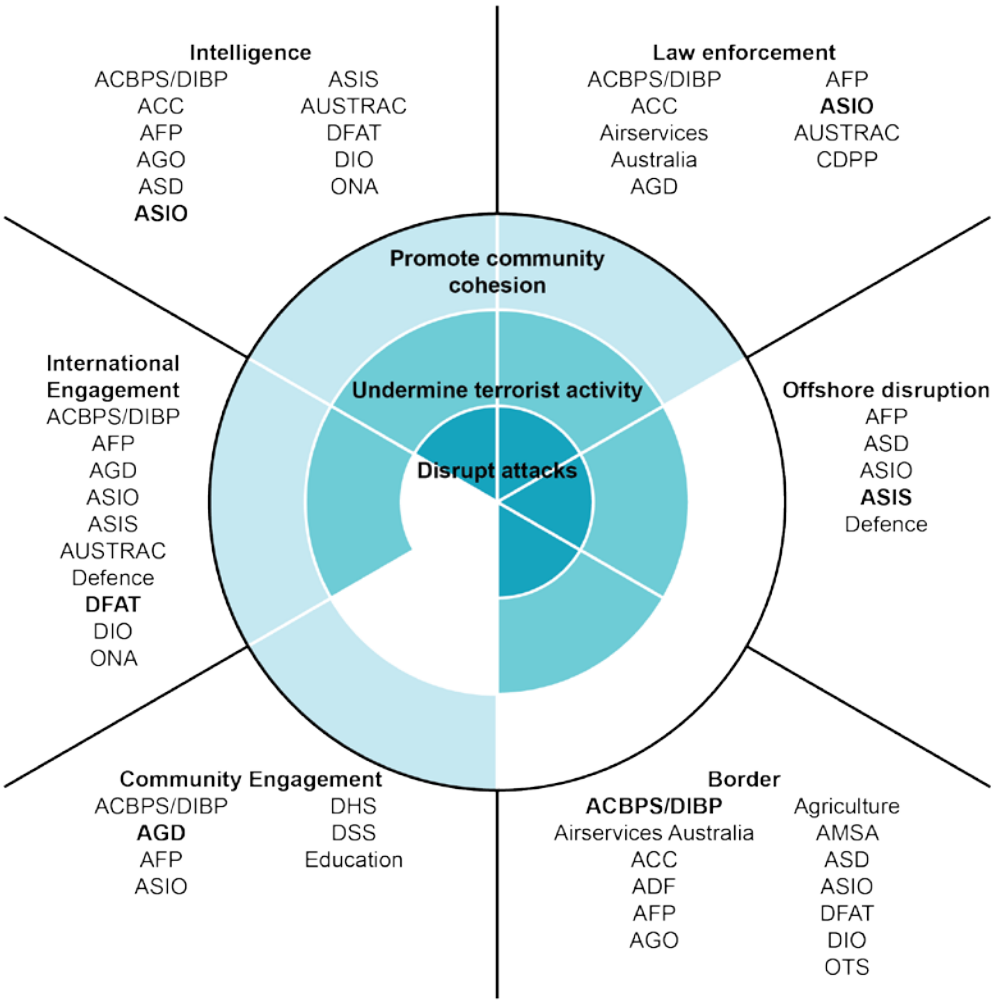


Source: ASIO.

In June 2006, Australian citizen Faheem Lodhi was convicted in the NSW Supreme Court of terrorist offences relating to planning a terrorist attack.

1 This unit was closed in early 2013.

Chart 5: Commonwealth CT functions and activities in 2014



Compare this Chart 5 to Chart 3 on page 9. Many more agencies are now involved in CT activities, supporting a much wider range of functions.

2008 – 2011

The 12 coordinated shooting and bombing attacks over four days in 2008 in Mumbai and the 2009 bombings of the Marriott and Ritz Carlton hotels in Jakarta further fuelled regional and global concerns. However, other major plots, such as the al-Qa'ida in the Arabian Peninsula's (AQAP) plot to blow up an UPS aircraft on route, were foiled, providing some confidence that new CT measures were working.

In Australia, the sense of progress was reinforced by a series of successful prosecutions and convictions. To build on these successes, agencies focussed on improving coordination of both policy and operations.

In 2008-2009, the Government enhanced Australia's national security framework by establishing:

- the Crisis Coordination Centre, an all-hazards facility within the Attorney-General's Department (AGD) to enhance whole-of-government situational awareness during a crisis
- the National Security College, which focuses on executive leadership, learning and development to enhance the functioning of the national security community.

In 2010, the Government delivered a Counter-Terrorism White Paper. This led to the establishment of the Counter Terrorism Control Centre (CTCC), a multi-agency coordination centre within ASIO, which prioritised and evaluated CT investigations.[2]

The impact and significance of terrorist use of technological advances became more pronounced.

- In 2007 and 2008, a software program enabling effective email encryption, Mujahideen Secrets, was released to al-Qa'ida (AQ) supporters.
- In 2010, the first issue of 'Inspire' magazine was published. The magazine was a significant shift from AQ's previous propaganda efforts. It was published online, in English, and promoted simple attacks by individuals using commonly available items as weapons.

The 2008 Smith Review of Homeland and Border Security considered these roles, responsibilities and functions of Commonwealth departments. While it had implications for our CT arrangements, it was focussed more broadly on national security.

- The Review recommended against the creation of a Homeland Security-style department which would have brought together a greater number of operational agencies. Instead, the Review recommended a range of measures to improve coordination and strategic planning.
- The Government responded to the Review by establishing the position of National Security Adviser within the Department of the Prime Minister and Cabinet (PM&C) to improve strategic direction and coordinate policy development and crisis response.

In 2010, the Commonwealth launched the inaugural Countering Violent Extremism (CVE) programme, addressing factors that make people vulnerable to extremist influences and recruitment by terrorists. The emphasis was on prevention and early intervention.

Convictions were achieved as a result of Operations Pendennis (14 convictions in 2009) and Neath (three convictions in 2010).

The Independent National Security Legislation Monitor (INSLM) was established in 2010 to review the operation, effectiveness and implications of Australia's national security legislation on an ongoing basis. This includes considering the adequacy of safeguards for the rights of individuals.

2012 – 2015

The most recent three year period has largely been shaped by developments in the Middle East. The Arab Spring uprisings and the destabilisation of a number of Middle Eastern and North African states have created physical and ideological space within which terrorist and extremist groups have found greater freedom to operate. These terrorist groups have unprecedented appeal and reach into Australian communities.

Coinciding with these developments, and potentially drawing inspiration from extremist propaganda released since 2010, there has been a rise in small-scale terrorist attacks. These include the Boston bombing, the knife attack on two police officers in Melbourne, the attack on the Canadian Parliament, the Charlie Hebdo attack and the Porte de Vincennes hostage crisis in Paris.

The most recent events in Martin Place have tragically confirmed the risks.

In Australia, further legislation has been introduced to enable agencies to keep abreast of the threat.

- On 30 October 2014, the Government introduced the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 into Parliament. If passed, it will require Australian telecommunications companies to keep a limited set of metadata – information about the circumstances of a communication – for two years.
- On 3 November 2014, the *Counter-Terrorism Legislation Amendment (Foreign Fighters) Act 2014* received Royal Assent, amending 22 Acts to respond to the threat posed by Australians engaging in, and returning from, conflicts in foreign states. The legislation strengthened

2 In 2014 the CTCC was replaced with the Australian Counter Terrorism Centre, with an expanded mandate.

- Australia's ability to arrest, monitor, investigate and prosecute returning foreign fighters and onshore extremists.
- On 2 December 2014, Parliament passed the Counter Terrorism Legislation Amendment Bill (No. 1), which responds to urgent operational requirements identified by law enforcement, intelligence and defence agencies.
- Further CT legislative reform will occur in 2015, including to address a number of the remaining recommendations of:
    - the COAG Review of CT Legislation, and
    - the INSLM's annual reports.

In 2014, the National Border Targeting Centre, comprising representatives from nine agencies, was established within the Australian Customs and Border Protection Service (ACBPS) to analyse and target high-risk passengers and cargo.

Also in 2014, the Government launched a new CVE programme, which includes a more direct approach to identifying and providing support to individuals at risk of radicalisation. An early intervention programme will complement the efforts of the AFP's National Disruption Group. The National Disruption Group will assist in managing the return of Australian nationals involved in conflict overseas.

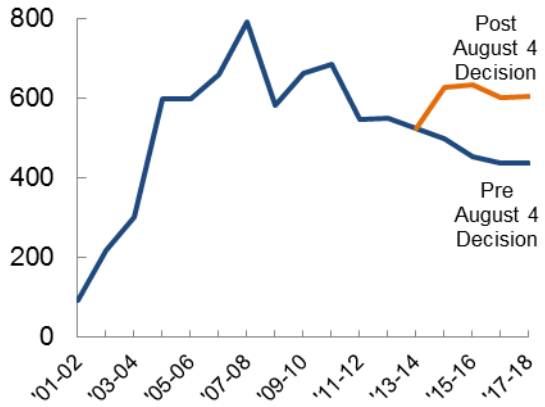
CT Resourcing Trends

It is difficult to disaggregate CT funding from broader national security funding. National security agencies resource their CT activities from a combination of funding from their base budgets as well as dedicated CT funding measures agreed by the Government.

As is outlined in Chapter 6, there was a significant rise in funding for national security activities from 2001-02 to 2009-10, with funding since then plateauing.

Likewise, there was a significant rise in dedicated funding measures for CT from 2000-01 to 2007-08, and a decline thereafter. This decline is projected to reverse due to the additional $632.3 million in dedicated CT funding agreed by the Government on 4 August.

Chart 6: Dedicated funding measures for CT, $ million



Source: Department of Finance.

Two: The threat environment

Key points

The major terrorist challenges of the last decade remain: hierarchical cells are still making detailed plans for mass-casualty attacks.

However, these challenges have now been joined by more mobile and agile threats.

Terrorist groups are successfully motivating attacks, often low tech and unsophisticated, by lone actors despite little or no direct contact between the organised group and the attackers.

For Australia, this trend manifests not only as an increase in the magnitude of the threat but also in its increasingly home-grown nature: we have more foreign fighters, terrorist supporters and terrorist sympathisers than ever before.

The challenges are exacerbated by the use of encrypted communications, and the increased prevalence of lone actor and small scale attacks.

The threat posed by global Islamist terrorism is growing and becoming more diverse. Perhaps the most striking example of this growth has been seen in the Iraq-Syria conflict zone. Here, the lethal convergence of ideological attraction and the geographical accessibility of the conflict has drawn foreign fighters on an unprecedented scale.

The declaration of a global caliphate, led by ISIL Emir Abu Bakr al-Baghdadi, has added to the allure of the extremist narrative. In declaring a caliphate, ISIL has appealed to the sense of nostalgia held by some for a period of Muslim dominance over large swathes of territory, stretching well beyond the Levant. The restoration of a caliphate has also been a source of great pride among some segments of the Islamic community.

Essentially, the conflict in this region has seen the creation of a new generation of increasingly capable, mobile, and digitally-connected terrorists with the ability to disseminate their extreme ideology around the world.

Beyond the escalated threat posed by the sheer number of fighters being drawn into conflict zones, an apparent evolution in terrorist tactics is also dramatically altering our threat landscape: terrorist groups are increasingly encouraging random lone actor attacks.

The concept of lone actor attacks is not new. However, as a tactic to avoid the attentions of security agencies and to spread panic, it is becoming more prevalent. Choosing this style of attack also broadens the pool of potential actors. A terrorist attacker need no longer be drawn from a limited pool of highly-skilled, centrally controlled and directed operatives. Instead, he or she could be anyone with mere intent, as the tools required for an attack – such as a car or a knife – are readily available.

Global evolution

Ongoing instability in the Arab world will continue to provide terrorists with increased room for

operations. The spillover from the conflict in Syria and Iraq will further exacerbate regional instability. The CT capabilities of many countries, especially in the Middle East, are being constrained by increasing areas of ungoverned space and multiple security issues.

While AQ was previously the focus of the West's CT efforts, the prominence of the AQ core has diminished. This is largely due to the loss of key personnel in ongoing targeted operations. For the moment, AQ core will focus on survival, but the organisation is resilient and capable of rejuvenation.

While AQ core may have been diminished, the overall extremist cause has been strengthened. The conflict in Syria and Iraq has changed the terrorism landscape and reinvigorated Islamist terrorists worldwide. Safe havens in Syria and Iraq, including the large tract of territory controlled by ISIL, are far larger and richer than earlier safe havens in Pakistan's Federally Administered Tribal Areas, or the Sahara where al-Qa'ida in the Islamic Maghreb (AQIM) operates. That gives terrorists significantly more territory and resources to defend, and state-like capabilities to marshal, thereby presenting a potentially more deadly adversary.

Unlike terrorist groups in other regions of conflict, the Syria-Iraq groups welcome reinforcements from around the world. Groups such as ISIL accept all comers who share their extreme Islamist ideology. As a result, there are more than 80 different countries represented among the ranks of foreign fighters in Syria and Iraq. So, even if the flow of foreign fighters to Syria-Iraq were to stop today, an international cohort of hardened jihadists has already emerged. They in turn will play a role radicalising and influencing others around the world.

Elsewhere in the Muslim world, notably parts of Africa, jihadists are opening new fronts and will continue to exploit instability. Terrorists are unlikely to seize control of any state soon – with ISIL's proclamation of its own state and its clear threat to Damascus and Baghdad as the exception.

Groups influenced by the terrorist narrative and in the orbit of ISIL and AQ further increase the terrorist threat. Many of these groups are under little or no CT pressure. Most will prioritise local fights, such as Al Shabaab's war with the Government of Somalia and African intervention forces or AQIM's skirmishes with Malian and other regional troops. But some of these groups will also attempt attacks in the West, or on Western interests in their areas of operation. Terrorist groups in areas such as Yemen and Somalia may continue to appeal to foreign fighters, including Australians – albeit on a smaller scale than Syria and Iraq.

Further attempts at mass-casualty attacks in the West are almost certain over the next few years: there is good reason to believe AQ-associated elements are planning such action now. But a mass-casualty chemical, biological, radiological or nuclear attack will likely remain beyond the reach of most groups.

Regional threats

Within our region, terrorists in Southeast Asia, particularly in Indonesia, will remain a malignant presence. Terrorist groups won't gain any real support from the vast majority of Muslims in the region, or threaten the stability of their governments, but they continue to rebuild capacity following crackdowns in the last decade.

Significant risks do endure in Indonesia. Australians are more likely to be targeted in terrorist attacks there than anywhere else overseas.

There are a significant number of Indonesian militants in the Syria-Iraq war. Fighters returning home to the region will inject capability and international connections into local networks. These elements were the two key ingredients in the 2002 to 2009 anti-Western bombing campaign, which saw several attacks on Westerners in Bali and Jakarta, including the deaths of 88 Australians in the 2002 Bali bombing.

At the same time as returning foreign fighters bolster the ranks of extremists, terrorists involved in anti-Western attacks over the last decade are being released from prison, for the most part unreformed and un-rehabilitated, compounding the threat.

Exploiting social media

The global reach of digital media has had a transformative effect on nearly every aspect of modern life. Terrorism is no exception. Groups such as ISIL are acutely aware of the power of social media, and are adept at exploiting it to promote

their message. Like other terrorist groups before them, various groups in Syria and Iraq have produced high-quality propaganda in a range of languages. However, the effectiveness of modern terrorist groups' propaganda is exponentially increased by the use of social media to ensure that their message is broadcast to a mass audience. Their material is broadly disseminated through social media – including mainstream platforms such as Twitter, and is no longer confined to password-protected dark corners of the online world.

Exploiting secure communication technology

It is not just the ability of terrorist groups to reach a mass audience that concerns national security agencies – advances in online security and encryption increasingly allow terrorists to communicate out-of-sight of intelligence agencies. ISIL and other terrorist groups are making greater use of secure communications platforms. Readily available technologies are giving terrorist groups an ability to forge cross-country links and to communicate with a global audience, protected by advanced encryption of the sort previously only available to states and major enterprises. The challenge of maintaining access to terrorists' communications is a pressing one for intelligence agencies.

Indeed, terrorists' usage of digital media has become so adroit that the United Kingdom (UK) Government Communications Headquarters Director Robert Hannigan has described the internet as 'the command and control networks of choice for terrorists'.

Low attack thresholds – 'lone actor' or self-initiated threat

While Australia continues to deal with plots to inflict mass casualties or major infrastructure damage, potential 'lone actor' attacks pose an increasing threat. These attacks involve individuals or small groups operating with little or no contact with traditional terrorist groups, but often inspired by terrorist groups' public calls for such acts.

Lone actor and self-initiated attacks in the West

March 2012: Toulouse and Montauban shootings. Mohammed Merah conducted a series of three gun attacks targeting French soldiers and Jewish civilians. Seven people were killed, and five were injured. Merah was shot and killed after a 30-hour siege.

22 May 2013: Murder of Drummer Lee Rigby. Michael Adebolajo and Michael Adebowale killed Rigby in a random attack on a British solider in Woolwich, London. They hit Rigby with their car before using knives and a cleaver to stab and hack him to death. They claimed to have killed Rigby in revenge for the killing of Muslims by the British military in the Middle East.

24 May 2014: Jewish Museum of Belgium shooting. French national Mehdi Nenmouche opened fire on civilians at the Jewish Museum of Belgium in Brussels, Belgium, killing four. He is believed to have spent time fighting in Syria before undertaking the attack.

23 September 2014: attack on police officers in Melbourne. Australian citizen Abdul Numan Haider attacked two police officers – one AFP and one Victorian Police – outside a police station in Melbourne. Haider stabbed both police officers before being shot dead.

20 October 2014: Quebec vehicle attack. Martin Couture-Rouleau deliberately hit two Canadian: military members with his vehicle, killing one and seriously injuring the other. He was shot and killed by police after a high-speed chase. Prior the attack, Couture-Rouleau had his passport seized as he attempted to travel to Turkey.

22 October 2014: Ottawa Parliament shooting. Michael Zehaf-Bibeau shot and killed a Canadian soldier at the National War Memorial before storming into Parliament Hill in Ottawa. He was killed by Parliamentary security during a shoot-out. Zehaf-Bibeau had expressed frustration over the difficulties he was having in obtaining a passport, and expressed sympathy with ISIL.

15 December 2014: Martin Place siege. Man Haron Monis took 17 hostages in a café in Martin Place, Sydney. Two hostages, and Monis, died in the siege. Monis stated his actions were an attack by ISIL in negotiations during the siege.

Such calls to action do not identify specific targets, but encourage potential terrorists to use their initiative to conduct small-scale attacks against any available targets using easily available materiel. These types of attacks can be characterised in a number of ways, including 'self-initiated' or 'low-threshold'. However, the term 'lone actor' is used in this report to include all such attacks.

Success – even in failure

It is not just the tactics of terrorist groups that have changed, their definition of 'success' has also changed. Previously, if an attack was thwarted or otherwise failed to reach its objective, it would have been considered a failure by security agencies and terrorists alike. But the goalposts have shifted. Now, terrorist groups even claim as victories those foiled attacks which have generated public fear, or increased cost or inconvenience to their targets. For example, an AQAP 2010 'printer bomb' attack plan (explosives hidden inside printers carried via cargo planes) was foiled by intelligence. But AQAP still considered it to have been a success, due to the fear it provoked and the costs involved in the resulting changes to air freight screening.

Impact on community cohesion

In addition to the threat of terrorist attack, international conflicts framed as religious or sectarian in nature can resonate locally and add to or reignite tensions associated with longstanding communal grievances. Recent incidents range from verbal abuse and intimidation to arson attacks directed towards Shia businesses.

Key changes

In summary, while many elements of the terrorism threat have remained constant, the following changes pose significant challenges to national security agencies:

- the increased scale of the threat
- the home-grown aspect
- lower barriers of entry to terrorist groups
- lone actor attacks
- use of everyday items as weapons
- individuals can move rapidly from intent to attack
- social media
- secure and encrypted communications.

While any of these elements on their own would constitute a significant challenge to Australia's CT efforts, their convergence places unprecedented strain on agencies working in this field.

Three: Performance of Australia's counter-terrorism arrangements

Key points

Existing CT arrangements have performed well. However, there can be no room for complacency.

The key challenges we have faced over the last decade remain and in many cases have become more difficult to address.

The threat of terrorism in Australia is rising and it is harder to combat. Many of the metrics are worsening: the numbers of foreign fighters, known sympathisers, supporters, and serious investigations are all growing.

To meet the rising threat, more can be done to ensure agencies maintain a competitive technological edge, work together seamlessly and degrade ideological support for terrorists.

The Review examined the effectiveness of our current CT arrangements in terms of the outcomes achieved, strengths and challenges. Overall, the Review assesses that our current CT arrangements have performed well.

But there is a rising tide of Australian support for terrorist groups and direct involvement by Australians in their violent activities. This rising tide presents a growing challenge for all of Australia's national security agencies.

The outcomes of Australia's CT efforts

Disrupting terrorist attacks

The overarching objective of Australia's CT arrangements is to keep Australians safe from attack. Since 11 September 2001, Australian security and law enforcement agencies have collaborated to disrupt the terrorist activities of numerous individuals and a number of larger-scale plots. This has resulted in 35 prosecutions and 26 convictions for terrorism-related offences.

There has not been a large scale terrorist attack in Australia this century. The attack by Numan Haider on two police officers in September 2014, and the Martin Place siege in December 2014 were the only successful terrorist attacks or incidents on Australian soil.

Undermining terrorist support and activity

On the whole, efforts to detect and undermine terrorist support have been effective despite increasing volume, complexity and significance of the matters involved.

Attempts to stem the flow of Australians travelling abroad to fight with terrorist groups in Syria and Iraq (and prior to 2010, Afghanistan and Somalia) have been significant in undermining terrorism support.

Since 2011, the number of passport cancellations has been increasing exponentially, reducing the flow of Australian fighters supporting terrorist groups.

Terrorist plots disrupted since 2001

2003-04: Investigation of Faheem Lodhi found he was plotting to bomb the national electricity grid or defence sites; he was convicted of terrorism offences.

2005: Nine individuals were arrested in Sydney after sourcing chemicals and materials for use in the preparation of an explosive device; possession or attempted purchase of firearms and ammunition; and possession of large quantities of extremist material. All were convicted of terrorism offences.

2005: 13 individuals arrested in Melbourne and charged with plotting mass casualty attacks, with the intention of coercing the Australian Government to withdraw from Iraq. Nine individuals were convicted of terrorism offences.

2009: Five men charged with conspiracy for preparation for an attack using firearms on Holsworthy Army Barracks in Sydney. Three were convicted.

2014: In response to intelligence revealing an alleged plot to kill a random member of the public, entry and search operations were conducted on multiple occasions in Sydney.

Longer term, passport cancellations reduce the growth in the number of Australians who have developed combat skills and undergone further ideological inculcation on the battlefield. Keeping radicalised individuals onshore does, however, present long-term investigative challenges for law enforcement and intelligence agencies.

Blocking the flow of terrorist support

There have been successes in disrupting terrorist financing and recruitment and in working with other countries to deny terrorists access to goods and materiel.

Since the start of the civil war in Syria, the Australian Transaction Reports and Analysis Centre (AUSTRAC) has blocked funds to certain terrorist groups, including de-registering four international money transfer organisations suspected of channelling funds to terrorist groups.

Key recruiters have also been identified and their networks have been disrupted to further restrict the number travelling overseas to support terrorist causes.

Blocking facilitation networks

In 2013, a Sydney-based man was arrested in Sydney and charged with facilitating the recruitment of Australians to train and/or fight with terrorist groups in Syria, including Jabhat al-Nusra. He is one of a growing number of recent arrests for 'home-grown' facilitation.

Impeding the development of terrorist capability

The first step in impeding the development of terrorist capability is to identify changes in the threat environment and detect shifts in terrorist methodologies. Agencies have identified recent shifts early and prepared accordingly.

By mid-2012, ASIO had already reported on the possibility of inter-communal violence in Australia resulting from the Syrian conflict. It had also identified Australians who had departed Australia to participate in the Syrian conflict and warned of the development of terrorist capability associated with this travel.

Agencies have heeded the growing threat and redeployed resources to impede further development of terrorist capability. In August 2014, the ACBPS established CT teams at eight major international airports. These teams have now conducted nearly 1,870 physical examinations or interventions at the border.[3] The physical examinations and interventions have located evidence of movements of – or attempted movements of – large sums of cash and seen the confiscation of violent extremist material.

Australian agencies have also worked with our international partners to disrupt terrorist activity overseas.

[3] Figure accurate as of mid-November 2014.

Degrading ideological support for terrorism

Intelligence agencies have engaged with individuals at all levels within communities to diminish support for violent extremist ideology. This engagement has also provided an avenue for community concerns regarding terrorist activity to be raised.

The Commonwealth also leads more formal CVE efforts to degrade ideological support for terrorism.[4] This focuses on activities to challenge violent extremism through education and training, skills building, leadership and mentoring, development of counter narratives to challenge violent extremist ideologies, as well as a number of online media projects.

In addition, the Commonwealth has partnered with state and territory governments to fund a range of short term initiatives to:

- support the rehabilitation of people imprisoned for terrorism related offences
- prevent the radicalisation of other prisoners
- conduct joint research with academics to build Australia's understanding of violent extremism and the most effective ways of countering it.

Promoting community cohesion

Building community cohesion and resilience to violent extremism is an important component of Australia's CVE strategy. Agencies have actively engaged and raised community awareness of:

- the legal consequences of travelling to fight in overseas conflicts
- the personal impact for those participating or supporting participation, and the impact on their families
- Australia's foreign policy position
- how the Australian Government is providing development assistance and humanitarian aid to those affected by the conflicts
- alternative options for communities to support those affected.

Government agencies promote community cohesion for Australian society as a goal in its own right. This work also addresses underlying factors which can lead to radicalisation such as social and economic disadvantage.

Current strengths of Australia's CT efforts

Operational effectiveness

National security agencies have identified and prevented terrorist attacks and disrupted facilitation networks. Developing threats have been identified early, and advice has been disseminated broadly and quickly across government through a range of formal and informal methods.

Mechanisms, such as the Joint-Counter Terrorism Teams and the Counter-Terrorism Control Centre, allow agencies to de-conflict operational activity, limit duplication and ensure resources are directed to mitigate the highest CT threats.

Strong frameworks and trust between agencies has ensured they react rapidly to deliver a coordinated response to any threat.

Operation Appleby

In the recent Appleby operation, once the threat had crystallised, agencies moved rapidly from investigation to disruption, mobilising up to 800 law enforcement and intelligence officers in multiple states within a 36 hour time frame.

Protocols have enabled information sharing between commonwealth and state police and intelligence agencies. Operational outcomes are enhanced by joint training, sharing of operational resources and interagency secondments which build relationships and increase interoperability with partner agencies.

[4] CVE is the banner used to describe efforts of Australian governments to prevent processes of radicalisation leading to violent extremism, including terrorism, and where possible to help individuals disengage from a preparedness to support or commit acts of violence to achieve political, social or ideological ends.

Australian Defence Force support to CT operations

While ADF operations overseas have not traditionally been framed as part of Australia's CT mission, they have contained significant CT elements. For example, the purpose of Operation SLIPPER in Afghanistan was 'to ensure the country does not again become a safe haven from which terrorists can plan attacks on Australians'. Currently, Operation OKRA, the ADF contribution to the international effort to combat the ISIL terrorist threat in Iraq, is also specifically intended to achieve a CT outcome.

Consequently, ADF requirements for intelligence for Operation OKRA significantly overlap with everyday CT work done by Australian national security agencies. That said, ADF requirements will be particularly high priority and time sensitive, due to the operational and tactical nature of ADF missions. Importantly, the ADF is not solely a recipient of intelligence support: ADF missions may also provide valuable intelligence on CT issues and developments, and this needs to be factored into CT prioritisation and coordination measures.

Stronger collaboration

Interagency collaboration has been built progressively and is stronger now than ever. There are a range of ad hoc and permanent arrangements that help agencies work across traditional agency and functional silos.

In particular, the Australia-New Zealand Counter-Terrorism Committee (ANZCTC) provides a mechanism for multi-jurisdictional information sharing, national capability development, and collaboration to prevent terrorism within Australia.

International partnerships are used to enhance Australia's global reach and exchange critical intelligence.

Australia has strong operational partnerships with international counterparts both through the AFP and the intelligence agencies. Policy agencies also regularly engage bilaterally with international partners and through a range of multilateral fora to share best practice, build capacity and collaborate to counter terrorism.

Effective legislation

Australia has a strong CT legislative framework which has been regularly updated since 2001. These reforms have helped to ensure that national security agencies have the necessary capabilities to counter terrorism. Legislation introduced since 2001 has underpinned all 35 Australian prosecutions for terrorism-related offences.

Our CT legislative framework is balanced with a range of legal safeguards, including:

- clear ministerial accountability
- parliamentary oversight provided through the Parliamentary Joint Committee on Intelligence and Security (PJCIS)
- independent assurance by the Inspector-General of Intelligence and Security, who is responsible for providing advice to the Prime Minister, senior ministers and Parliament on whether Australia's intelligence and security agencies act legally and with propriety
- activities by INSLM to review the operation, effectiveness and implications of Australia's national security legislation on an ongoing basis.

Closer community engagement

Australia's CVE efforts have built closer relationships between Australian governments, academia and communities where individuals may be radicalised or at risk of radicalisation. Governments now have the ability to engage with previously difficult-to-access communities, enabling quick and effective information flows.

The CVE Programme also provides a banner for agencies to undertake activities in conjunction with communities without the more constrained public perceptions of direct engagement with intelligence and law enforcement agencies.

Challenges and weaknesses

The key threats we have faced over the last decade remain and are growing. The evolution of terrorist behaviour and methodologies, including advances in communications and digital media, mean the threats have become more difficult to address.

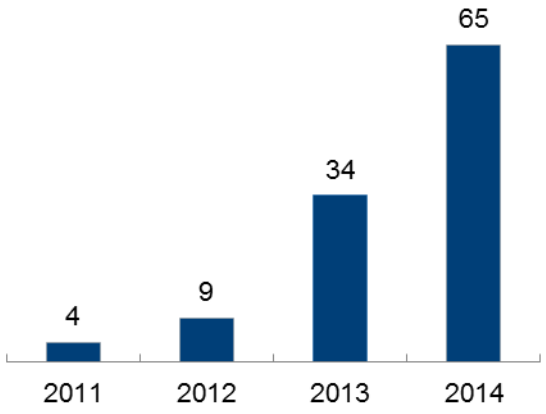
Australia's CT efforts until now have been largely reactive – agencies have responded to threats as they have emerged. With the successes in dealing with major threats, coupled with pressure on funding, the national security community tended to focus on major plots at the expense of seemingly lower priority issues and some strategic concerns.

This in part contributed to the community not being ideally positioned to address the sudden emergence of extremist groups in Syria and Iraq – and the extent of these developments' resonance in Australia. This was compounded by the scale of the emerging challenge and structural issues within the community.

The rising tide

The rapidly growing scale of the threat and its increasingly complex nature, including an increasing proportion of suspects who were previously unknown to authorities, is placing greater pressure on the technical and physical resources of agencies.

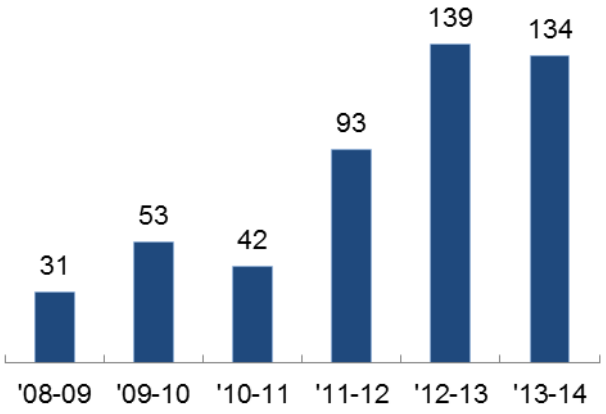
Chart 7: Number of passport cancellations



Source: ASIO

Prior to 2000, ASIO had never recommended the Minister for Foreign Affairs cancel a passport to prevent the travel of an individual of terrorist-concern. In 2013 and 2014, ASIO issued 99 adverse security assessments recommending the Minister for Foreign Affairs cancel (or refuse) passports on security grounds.

Chart 8: Suspicious Matter Reports assessed by AUSTRAC as relating to terrorism financing



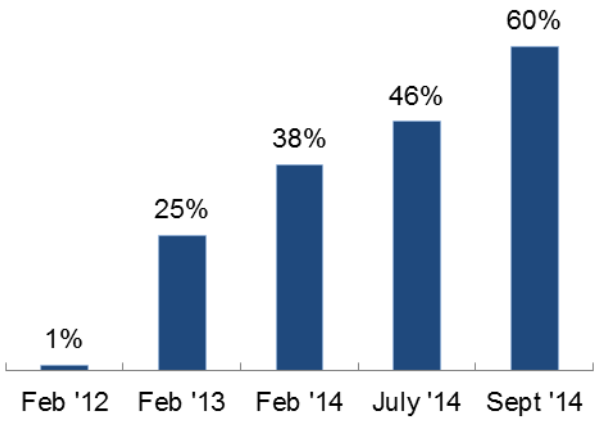
Source: AUSTRAC

Other indicators show a similar trend. For example, the sharp increase in the Suspicious Matter Reports relating to terrorism financing reported to AUSTRAC could be an indicator of increased financing of terrorism.

So, the scale of the threat is increasing and, in general, terrorist plots are offering less lead time and therefore less opportunity for disruption. Against this background, agencies have no choice but to discharge their obligations to protect public safety by taking overt but often short term disruption activity to prevent imminent attacks. This overt activity limits law enforcement's ability to gather the evidence necessary to support a successful prosecution.

In the absence of a prosecution, radicalised individuals are returned to the community feeling more disaffected and with an improved tactical awareness of national security agency capabilities and knowledge. Typically, they would not be deterred from the intent to commit a terrorist act but they are aware they are being surveilled and so are being more careful and harder to monitor. Investigations, particularly because they don't result in prosecutions and the closing of cases, are actually increasing in volume and complexity. Indicators of the increase in scale and complexity can be seen in the rapidly increasing number of investigations ASIO categorises as being 'priority investigations'.

Chart 9: Per cent of total ASIO CT investigations categorised as 'priority' investigations



Source: ASIO

Challenges at the border

Since terrorism operates globally, border agencies have a critical role in identifying and preventing instances of terrorist-related activity.

Border agencies' CT responsibilities have traditionally focussed on individuals entering Australia. While this will remain challenging, the lure of the conflict in Syria and Iraq now requires an increased focus on individuals – including Australian nationals – departing from Australia.

The challenges of even identifying, let alone stopping, all potential Australian foreign fighters are illustrated well by the ability of convicted terrorist Khaled Sharrouf to depart Australia for Syria using his brother's passport. A number of other Australians have also been able to depart without attracting any attention.

A number of factors have been identified as contributing to border failures: the rapidly growing scale of the threat; the prevalence of previously unknown individuals; the measures terrorists are taking to thwart CT efforts; and some weaknesses in information sharing among CT agencies.

Australian agencies have also failed to adequately address community concerns around the ability of so-called 'hate preachers' to travel to Australia.

Maintaining a competitive advantage

Countering terrorism has always been an expensive and complex business. The speed of technical innovation and the ongoing consequences of Edward Snowden's revelations are making the task of maintaining a technological 'edge' over terrorists more difficult.

For example, the proliferation of communication platforms and encryption technology makes it difficult to maintain the expertise and access needed to detect and monitor terrorists' communications.

While much valuable intelligence is hidden by encryption, agencies also need to manage the volume of unencrypted metadata being created. More generally, the challenges of managing and exploiting this data requires investment in new and unique tools, skills and innovation.

It is worth noting that post-Snowden, relationships between intelligence and business have been strained, making it harder to access key data without legal compulsion. Terrorist groups also have a greater knowledge of the technological capabilities of national security agencies, making it easier to evade surveillance and monitoring efforts. Agencies need to use increasingly intrusive and sophisticated monitoring measures.

Information exchange

The ability to rapidly share important information is critical to countering terrorism. Currently, there are various technical and policy issues that make it hard to share information between relevant agencies. Some information technology systems are not compatible and agencies working to differing legislative mandates and requirements may be subject to restrictions that prevent them sharing information easily – particularly information related to Australian nationals.

The internet facing systems of agencies are accredited to different levels which means email connectivity is not universal. This slows down information sharing which is a particular problem in times of crisis. Sharing information with states and territories, as well as with our international partners, can also be complicated when Commonwealth systems are not compatible with the standards and security measures of other jurisdictions' systems.

Successive reviews have highlighted information sharing as critical across all areas of national security. The Cousins Review into border systems

to prevent Australians from travelling to join terrorist groups is the most recent example. While information sharing has improved in recent years, the problems are far from solved.

Degrading ideological support for terrorist activities

The increased threat of home grown terrorism has changed the landscape for Australia's domestic CVE efforts. Terror groups are running increasingly sophisticated propaganda campaigns and social media is affording them a broad and dynamic reach into vulnerable cohorts.

The rapid increase in the scale of direct threats is a result of increasing ideological support for violent extremism within parts of the community. To manage this long-term increase, we must degrade the ideological support so that we shrink the potential pool of terrorists and facilitators. Current CVE efforts are likely to be having some impact but more needs to be done – not all priority individuals, areas or organisations are being addressed.

However, even highly effective CVE programmes cannot provide complete insurance against radicalisation and extremism in our communities. This is especially the case in the face of particularly significant international developments – such as the rise of extremist groups in Syria and Iraq, and ISIL's declaration of a caliphate.

Meeting our challenges

The challenges associated with the evolving threat must be addressed if we are to achieve continued success in countering terrorism.

Potential ways to achieve the changes needed to effectively combat the threat are more comprehensively addressed in Part Two:

- Chapter 4: Cross-agency leadership and coordination:
- Chapter 5: Countering violent extremism
- Chapter 6: Resourcing pressures
- Chapter 7: National terrorism advisories for the public

Part Two:
OUR RESPONSE

Four: Leadership and coordination

Key points

Australia's CT effort relies on all relevant agencies working seamlessly together.

Using Operation Sovereign Borders as a model for whole-of-government cooperation, the Review considered how best to achieve an OSB-like 'effect' to counter terrorism.

The Review concluded that the foundations of our existing arrangements are robust and don't require structural change.

However, agencies would benefit from clear direction for CT efforts and further strengthened coordination mechanisms. The Review concluded that a senior official should be designated the National CT Coordinator. Options are:

- *the Director-General (DG) of Security*
- *a new senior position in the Attorney-General's Department*
- *a senior position in the Department of the Prime Minister and Cabinet.*

To deliver in this role, the National CT Coordinator should chair a new Senior Executive Counter-Terrorism meeting and be supported by a whole-of-government Australian Counter-Terrorism Centre – a cross-agency body perhaps best located within ASIO which already has suitable facilities.

As outlined in Chapter Three, the evolving terrorist threat environment is challenging the Commonwealth's CT capabilities as never before. It is therefore imperative that all agencies with CT capabilities work together seamlessly.

Operation Sovereign Borders (OSB) is a case study in how to tackle a clearly defined policy problem effectively requiring a whole-of-government response. The lessons that should inform an effective model to counter terrorism are the need for:

- clear and consistent political direction
- ministerial and senior executive accountability
- close cooperation and communication at the strategic decision-making level.

In considering how best to achieve an 'OSB effect', the Review examined how other comparable countries arrange their national security bureaucracies, and considered whether the creation of a new national security department would assist Australia's CT effort.

Based on conceptual and structural considerations, the Review concluded that the creation of a new department is not a necessary or practical way to strengthen our coordination of CT activities. However, existing coordination mechanisms should be strengthened to **ensure that all agencies are working in the closest possible harmony** at the strategic decision-making and operational levels.

It is important to note that ensuring the Commonwealth's CT efforts are well coordinated is only one part of a successful national CT approach. States and territories are responsible for a significant proportion of our national CT capability, so we must ensure the Commonwealth's arrangements dovetail seamlessly with state and territory approaches. Regardless of proposed Commonwealth governance changes, the ANZCTC is the most appropriate body to ensure the national CT effort is coordinated.

International comparisons

Other countries organise their national security agencies in different ways. The United States has adopted a centralised, 'super-agency' model where many functions are consolidated into a single agency. Canada has done the same thing – though to a lesser degree. The UK has taken a different approach. While some UK agencies have been consolidated (e.g. within the UK Border Agency), others retain their distinct roles but are subject to a degree of centralised coordination.

The Review concluded that there is no single international best practice model on which to base Australia's CT governance arrangements.

Do we need a Department of Homeland Security?

The 2008 review of Homeland and Border Security led by Mr Ric Smith AO PSM outlined the broad range of threats facing Australia. These included threats such as espionage and foreign interference, terrorism; natural disasters and pandemics. This 'all hazards' approach, combined with increased public expectations of the Government's response, led Smith to consider the merits of a Department of Homeland Security.

Smith considered a model where a single minister would be responsible for all domestic security-related elements of the Commonwealth. Proponents of the model have suggested that this would:

- improve national security governance
- better balance justice and law enforcement functions
- promote better cooperation and information sharing.

Improved national security governance

National security is dependent on the three main pillars working well together – military, diplomatic, and homeland security capabilities, enabled by intelligence. It has been argued that a more balanced allocation of ministerial and departmental responsibilities around these three main pillars could enhance the representation of national security issues within Cabinet.

Better balance of justice and law enforcement functions

Currently, the Attorney-General must balance his duties as first law officer of the Commonwealth with his national security responsibilities, including bringing forward measures restricting or even removing the rights of certain individuals.

Appointing a separate minister responsible for a Department of Homeland Security could free the Attorney-General to take a more unimpeded view of the legal ramifications and consequences of national security proposals.

Promote better cooperation and information sharing

There are two clear models for a national security department – a large 'super-agency' modelled on the US Department of Homeland Security or a small, coordinating Department of Home Affairs based loosely on the UK Home Office.

Insofar as CT is concerned, a 'super-agency' would likely be less, not more, responsive as large agencies tend to be less agile, less adaptable and more inward looking than smaller departments. Indeed, observers regularly remark on the US Department of Homeland Security's systemic problems in the areas of information sharing, partnerships and accountability.

The creation of a small, flexible, coordinating Department of Home Affairs reporting to a Minister for Home Affairs could avoid many of the drawbacks associated with bureaucratic gigantism. In the CT sphere, such a department would provide leadership and coordination to its portfolio agencies.

What could an Australian national security department look like?

Any new national security department would be responsible for a far greater range of issues than just CT. However, the broader merits of such a proposal have not been considered, as they sit outside the scope of this report.

This Review agrees with the conclusion reached by the Smith Review that a small, coordinating Department of Home Affairs could be effective at

leading Australia's CT effort if the department focussed on strategic issues.

A small Australian national security department could oversight all relevant domestic intelligence and law enforcement agencies – including ASIO, the AFP, and even agencies such as the Office of Transport Security. It might also include other smaller agencies such as the Australian Crime Commission, AUSTRAC, and CrimTrac. Alternatively, to retain a separation between intelligence and law enforcement agencies, ASIO could be left outside such a new portfolio.

Conceptually at least, such a department might also draw in elements of the Department of Immigration and Border Protection. However, those elements are currently in transition to the Australian Border Force (ABF). The emergence of the ABF is itself expected to generate a stronger CT capability.

Testing the idea of a Department of Home Affairs

This section considers the philosophy that underpins the existing structures of Australia's national security community, as well as the necessity and practicality of establishing a Department of Home Affairs. In particular, it focuses on ASIO and the AFP as the two largest operational players in the CT space.

The Attorney-General's oversight is key

In assessing the current arrangements for ministerial oversight of ASIO, the Review drew on earlier reviews, particularly the Royal Commission on Intelligence and Security conducted by Justice Robert Hope from 1974-1977.

Justice Hope concluded that the 'necessity for secrecy means that the normal processes of checks and balances cannot be applied' to ASIO, but that there was a clear need for Ministerial oversight of, and responsibility for, ASIO.

To Justice Hope, this role was an appropriate fit for the Attorney-General, a position best placed to balance the twin demands of security and civil rights.

The Attorney-General and ASIO: Importance of ministerial oversight

'… in respect of matters such as issuing warrants, the minister will obviously be required to adopt an entirely non-partisan approach, an approach which, as Attorney-General, he has to adopt in many of his other ministerial functions.'

and

'… he must keep himself sufficiently apart from the organisation so that he can see to it that the interests of the public, both in their rights and in security, are adequately protected.'

Justice Robert Hope – Royal Commission on Intelligence and Security, Fourth Report (1976)

The foundations remain relevant

Nearly four decades later, Justice Hope's findings are still relevant. Overall, the strong culture of oversight and accountability around ASIO has helped build and preserve public confidence in the organisation and in Australia's security and intelligence agencies more generally.

As ASIO's CT operational tempo heightens in the months and years ahead, public confidence in the Attorney-General's role as guarantor both of our security and our civil rights is an increasingly important asset in maintaining community confidence in our security services.

Indeed, it could be argued that the Attorney-General's dual-hatted role has played an important part in securing community and Parliamentary support for security-related legislation. Certainly, Australia has been able to introduce a broader, more effective suite of CT legislation than have other comparable countries. These legislative changes have been critical in maintaining and developing Australia's CT capabilities in the face of evolving threats.

The particular expertise of the Attorney-General by reason of these dual portfolio responsibilities promotes rigorous and integrated Ministerial consideration of security and individual rights and liberties, both in the authorisation of particular operations and in legislative and policy development.

Could the Attorney-General adequately oversee ASIO if it was in another portfolio?

The Review considered a scenario where the Attorney-General would retain responsibility for approving ASIO warrants – and implicitly protect against undue encroachment on civil liberties – even if ASIO was in another portfolio. In particular, the Review examined whether the Attorney-General's role approving Ministerial Authorisations issued in the Defence portfolio for the Australian Signals Directorate (ASD) and the Australian Geospatial-Intelligence Organisation (AGO) might provide a possible model.

Under existing arrangements, ASD, AGO (and ASIS) must seek authorisation from their own ministers for certain operations targeting Australian citizens. They must also seek the concurrence of the Attorney-General where those operations concern Australian persons who may be involved in activities that could pose a threat to security as defined in the *Australian Security Intelligence Organisation Act 1979 (ASIO Act)*.[5]

It is important to note that the Attorney-General's responsibility in relation to ASD, AGO and ASIS activities derives from his national security responsibilities as the Minister responsible for administering the *ASIO Act 1979*, not as First Law Officer. However, the Attorney-General relies on this dual hatted perspective on security and civil rights to assess the impact of individual warrant requests.

A minister solely responsible for ASIO would not be able to provide the same level of oversight on matters requiring a reconciliation of security and civil rights. Similarly, without a detailed understanding of operational activities, the Attorney-General would also be unable to provide adequate oversight and assurances that a proposed activity has proper regard to both security and civil rights considerations.

The occasions when the Ministers responsible for AGO, ASD and ASIS must seek the Attorney-General's concurrence represent a relatively small proportion of these agencies' activities given their focus primarily on *foreign* intelligence.

But given ASIO's activities focus more heavily on Australian citizens, the level of assurance the Attorney-General can provide in his oversight of operations is dependent on a well-developed understanding of the operational tools available. Separating operational oversight from the Attorney-General's portfolio risks breaking down this understanding.

The Attorney-General and the AFP

Even though law enforcement warrants are generally issued by a judicial officer or a nominated tribunal member appointed in a personal capacity, the AFP is nevertheless subject to and benefits from the Attorney-General's oversight.

A further example of the Attorney-General's oversight of law enforcement activities in relation to CT is the requirement that the AFP must obtain consent from the Attorney-General prior to making an application for an interim control order and also before commencing prosecutions for certain security offences. This includes prosecution for foreign incursions offences under Division 119 of the *Criminal Code Act 1995*.

Operational cooperation is well-established and effective

This Review also considered the relationship between ASIO and the AFP as a result of their collocation within the Attorney-General's portfolio. The relationship – including through the Joint Counter-Terrorism Teams located in all states and territories – has benefited significantly from collocation.

There are high levels of cooperation and mutual trust between the two organisations. Collocation has greatly enhanced Australia's international cooperation in building legal and law enforcement capacity in our region. Indonesia is a powerful example of where the two agencies – in cooperation with other relevant agencies – have agreed on an objective, coordinated efforts and achieved strong results.

While it would be possible for ASIO and the AFP to collaborate from different portfolios, the Review concluded that the collocation of these two agencies was a structural strength of the current system. There is no pressing rationale to interrupt the close, constructive way these agencies work together directly.

[5] This provision is provided for under the *Intelligence Services Act 2001*.

Similarly, the Street and Clarke inquiries stressed the importance of a close relationship between the AFP and the Office of the Commonwealth Director of Public Prosecutions, which has been greatly enhanced by collocation within the Attorney-General's portfolio.

Practical challenges establishing a Department of Home Affairs

There are also a range of practical considerations that suggest establishing a Department of Home Affairs would not be an optimal response to the terrorism threat to Australia.

- Australia's agencies with CT capabilities also perform a wide range of other functions – such as counter-espionage, or combatting drug-related crime. Putting these agencies together under the remit of a department with broad responsibility for domestic national security matters may leave our CT efforts in competition for attention and resources.
- A small department could struggle to gain traction leading a portfolio containing large, operationally focussed agencies with statutory independence such as ASIO and the AFP. The Smith Review came to the same conclusion.
- Given the CT threat must be addressed *both* through a domestic *and* an international lens, the consolidation of national security agencies within a Department of Home Affairs might lead to a tendency to privilege the domestic over the international elements of the problem. Such a tendency would be unhelpful in the current fluid threat environment.
- The creation of a new department – even on this limited scale – would involve disruptive change with the attendant risk of distracting from the CT task.

In respect of CT, this Review therefore concludes there is no compelling reason to change the current system of ministerial oversight and departmental structures. Rather, it should be retained and strengthened.

Better coordination of existing machinery of government

Our CT approach needs to be more consistently whole-of-government in outlook. We must ensure all relevant government departments and agencies bring their expertise to bear.

One way to achieve the increased cooperation that is needed in the Commonwealth's CT arrangements could involve either PM&C or AGD playing a more active role on the basis of a clear mandate and resourcing from Government.

However, this would not be the only option. Given the evolving threat environment, another model with some attractions would involve a new approach combining oversight of the Commonwealth's policy *and* operational activities by elevating the DG of Security to the key CT coordinating role.

The model developed to implement OSB has proven the value of a relatively small and agile coordinating body, led by a senior official acting as a single authoritative point of contact and accountability. The governance mechanisms put in place in August 2014, involving the establishment of a new centre bringing together all of the key Commonwealth agencies, are a positive step towards achieving the same effect.

The Review suggests that these arrangements be amended to:

- designate a leader for the CT community who would coordinate across agencies and support the Attorney-General in reporting to NSC
- provide for regular, focussed head of agency level engagement
- focus on strategic policy challenges and resolving impediments to CT coordination
- bring together all agencies from across government who can contribute to the CT effort.

Either the DG of Security, a senior official (Associate Secretary) in AGD or a similarly senior official in PM&C would be designated as the **National Counter-Terrorism Coordinator** (CT Coordinator). The CT Coordinator would be the most senior point of contact on CT matters. If the

CT Coordinator was the DG of Security or a senior official in AGD he (or she) would be responsible to the Attorney-General – who would retain ministerial oversight for the Commonwealth's CT efforts – and would support the Attorney-General in providing regular updates to NSC.

Establishing the position of CT Coordinator in AGD would build on the policy oversight of agencies such as ASIO, AFP and AUSTRAC which fall within the Attorney-General's portfolio.

If the CT Coordinator was based in PM&C he (or she) would report to the Prime Minister through the Secretary of PM&C. A National CT Coordinator based in PM&C would bring PM&C's traditional convening power to the role.

The CT Coordinator would also chair a regular secretary and agency head-level **Senior Executive Counter Terrorism Group** (Executive Group). The Executive Group's role would be to set the strategic direction and priorities for the Commonwealth's CT effort, and oversee the effective implementation of the suite of new CT measures endorsed by Government.

The newly constituted **Australian Counter-Terrorism Centre** (ACTC) – led by a senior official (for example at the SES Band 3 level) – would need to become a whole-of-government CT capability located within, but not as part of, ASIO. This distinction would be important in ensuring the ACTC remains credibly impartial, including for its evaluation of agencies' performance.

The ACTC's focus should be on progress against priorities and overcoming impediments to an effective CT approach. It would need to take on an important role in the **coordination** of strategic CT policy across the Commonwealth. But its focus should be on ensuring departments and agencies bring their expertise to bear in developing and implementing policy solutions, rather than taking on a role that is properly performed by an existing department or agency.

Chart 10 displays the proposed governance arrangements for the Executive Group and the ACTC.

It is imperative that Commonwealth CT efforts align with arrangements in the states and territories. To help ensure this, the Executive Director of the ACTC should seek membership on the ANZCTC. This would help to provide a level of shared visibility and accountability between the two bodies, as well as a strong connection to the Executive Group.

A clear statement of objectives

The OSB experience shows the importance of establishing a clear mandate for agencies to work to. To this end, the Review recommends that Government, through the ANZCTC, develops a new national CT strategy given the changes in the threat environment. This could be supported by the Prime Minister delivering a clear statement on Australia's CT objectives and priorities. The statement would focus on setting out the Government's strategic level objectives and priorities for promoting community resilience, disrupting terrorist networks and preventing attacks.

Table 1: Factors contributing to the success of OSB – Lessons for the ACTC

Key factors determining success	OSB	EG/ACTC
Implemented on basis of clear government policy	√	√
Comprised of representatives from a wide range of agencies	√	√
Senior-level attendance at key coordination meetings	√	√
Task groups allocated substantial responsibilities, led by senior officials	√	√
Reports regularly to agency head/deputies reference group	√	√
Regular cabinet reporting ensures continued ministerial attention/priority	√	√

Recommendations

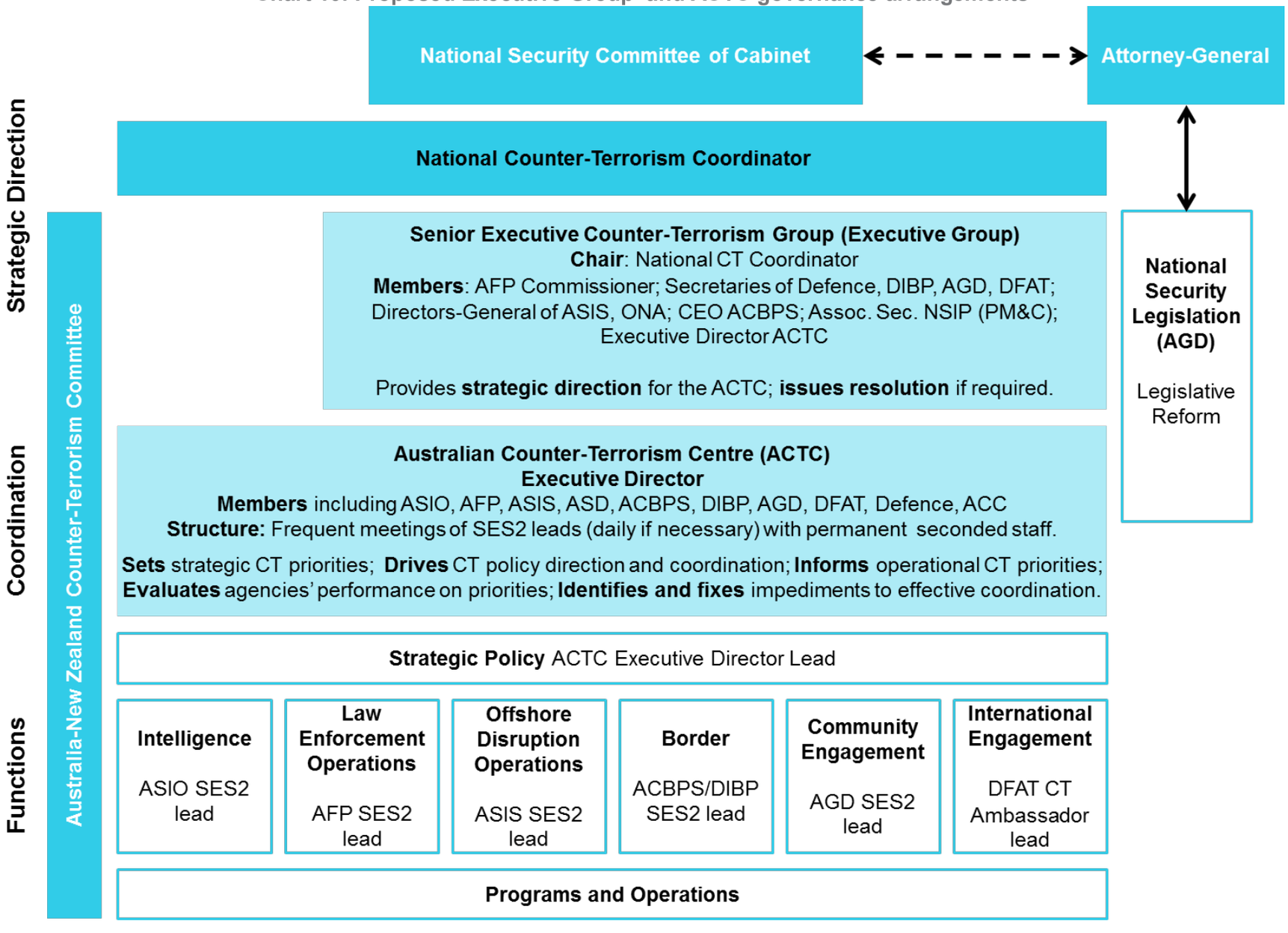
1. The Government, in close consultation with states and territories through the ANZCTC, develop a new national CT strategy which appropriately coordinates and balances our efforts to counteract the various threats we face, including from home-grown lone actors and radicalisation in our community.
2. The Government implement the following arrangements to provide strong, clear and co-ordinated leadership to ensure agencies respond effectively and appropriately to terrorism:

a. designate a senior official as the National CT Coordinator.

b. establish and expand an Executive Group at the Secretary/Agency Head level, chaired by the CT Coordinator, to set the strategic direction for the Commonwealth's CT efforts

c. mandate that the Australian Counter-Terrorism Centre draw together policy and operational agencies, including secondees from the states and territories, to work together closely on operations, policy challenges and capability development.

Chart 10: Proposed Executive Group and ACTC governance arrangements



Five: Countering violent extremism

Key points

There is no short term solution to the evolving terrorist challenge facing Australia.

Protecting Australians will always be the Government's top priority, and work to achieve this will necessarily at times have a short-term operational focus within the CT sphere.

However, to address the long-term implications of this challenge, we must put much greater effort into reducing the pool of potential terrorists.

To achieve this, the Government needs to boost its efforts to counter violent extremism by:

- *increasing Australia's national commitment to this work*
- *establishing community and public-private partnerships to better reach at-risk or radicalised individuals*
- *challenging extremist narratives*
- *addressing the underlying causes of violent extremism.*

Our efforts in this area have not yet been effective.

All of the metrics we have on the terrorism threat to Australia are worsening. We have a growing number of foreign fighters, terrorist sympathisers and supporters.

With operational agencies confronting unprecedented risk, we need to limit and reduce the pool of potential terrorists. Without this mitigation, resource pressures will continue to grow.

Work to counter the ideological attraction to terrorism has a shorter history than our operational efforts, with Australian governments agreeing to the first national CVE framework (Chart 11) in December 2009.

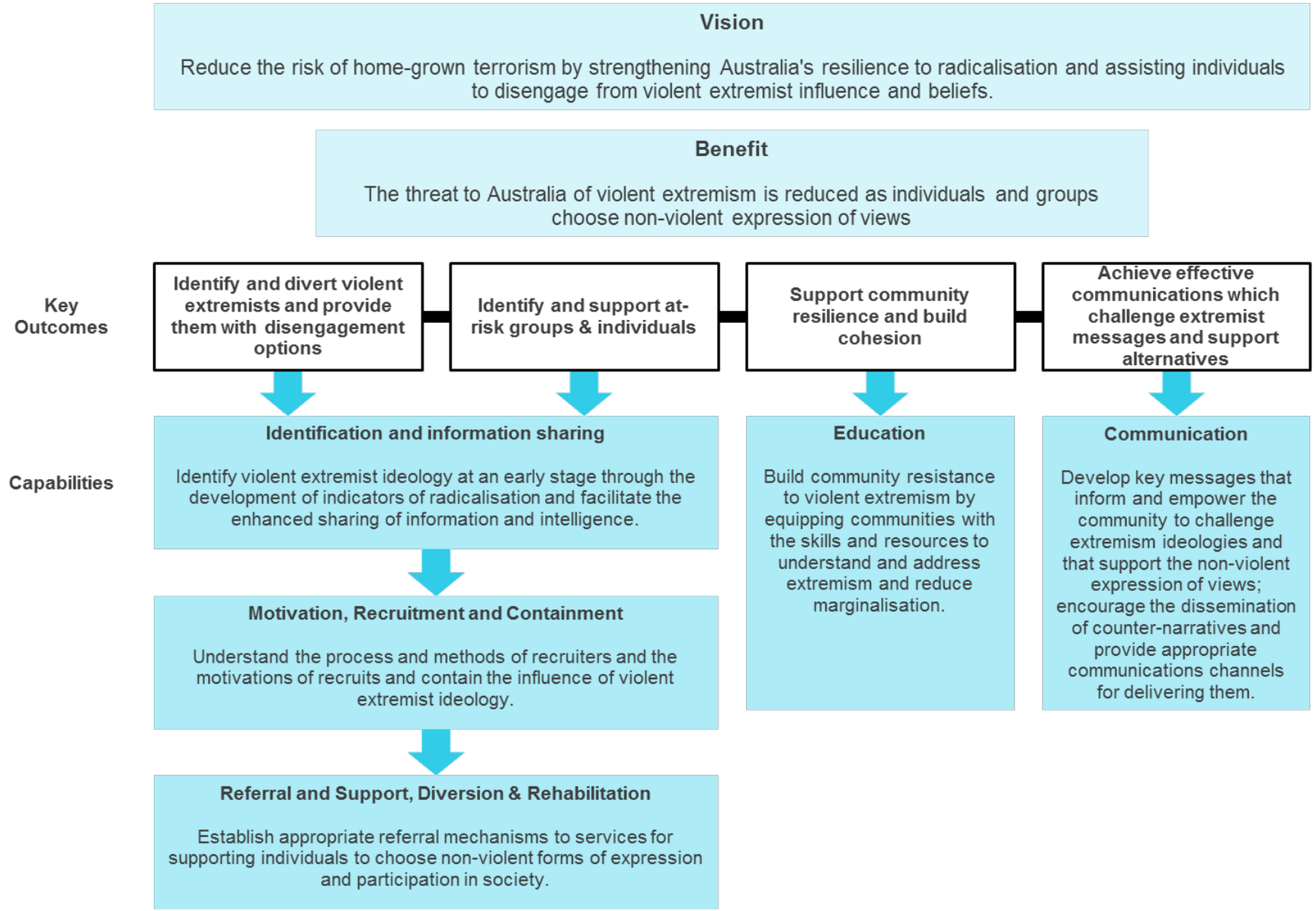
CVE efforts to date

Much of the work to date has been to strengthen relationships between the Government and communities at risk of radicalisation to violent extremism. This has included funding small-scale community activities to build resilience to violent extremism. These are activities such as:

- mentoring for youth vulnerable to extremist influences
- intercultural and interfaith education in schools
- online resources and training.

Not all of these programmes have been successful. Some of the efforts may also have been somewhat piecemeal or short term. In summary the programme of activities did not constitute a comprehensive approach to all priority individuals, locations and organisation.

Chart 11: National CVE Framework



In August 2014, the Government announced a new CVE programme, based on three core pillars of activity:

- tailored intervention programmes to connect at-risk individuals with a range of services to assist them to disengage from violence
- education and engagement activities to build resilience to violent extremism through well-informed and equipped families, communities and local institutions
- work to engage in the online environment.

The key focus is on diverting individuals from violent extremism. Activities designed to build cohesive and resilient communities have not of themselves proven to be sufficient to stop all individuals heading down a pathway of radicalisation. Individuals within these communities are still being drawn towards extremist ideologies.

The new CVE programme will deliver tailored intervention programmes to individuals. This will be done by identifying, assessing and referring individuals to support services that encourage them to reject violent ideology. The services available will include healthcare, mentoring, employment, education and counselling.

The community will be key in delivering these programmes.

- Community members and families will be most likely to notice indications that someone may be radicalising to violent extremism and to reach out to them.
- Community-based, non-government and local government organisations will be important service providers, delivering intervention services to individuals.

The Government is also exploring an expansion on its existing community awareness training initiatives to deliver more specific capacity-building programs to family and friends of at risk individuals as well as to community leaders so that they are able to challenge and counsel at risk individuals.

The need for a stronger mandate

The national CVE strategy is now five years old. Forward resourcing for this work is also relatively modest. Roughly $7 million per annum over the next four years is allocated to CVE-related Commonwealth and ANZCTC measures.

The strategy should be updated and endorsed by COAG to establish a clear political commitment to this work. The updated strategy should also consider the need for increased CVE joint resourcing across the Commonwealth and state and territory governments.

Based on international best practice, particularly the more mature efforts of the UK, a new CVE strategy should include measures to:

- better partner with communities and private sector partners to reach at-risk or radicalised individuals
- prioritise broader community cohesion efforts to address the social and economic causes of violent extremism
- challenge the reach of extremist narratives in Australia.

Community and public-private partnerships

Organisations that interact directly with radicalised individuals or those at risk of radicalisation are important in the fight against violent extremism. This includes schools, religious institutions, the mental health sector and jails. It will also be critical to partner with private sector organisations that can assist our efforts like Google and Twitter.

- Engagement with education and youth sectors, such as through sporting clubs and schools, is critical. These organisations are best placed to identify and divert young people from radicalisation.
- Faith leaders and peak groups can credibly engage their communities on ideological and religious issues. Many have expressed a desire to be at the forefront of work to tackle radicalisation.

Getting the most out of our partners

Opportunities to partner with community and private sector organisations on CVE are diverse, and could include: media training and capacity building by social media providers like Facebook and Twitter to hep community organisation to improve their digital literacy and reach to at-risk individuals.

- Companies such as Google and Facebook are important because violent extremists use their services, promoting their message to at-risk individuals. Companies have a responsibility to remove this material, but can also provide a platform to promote alternative messages and can provide important insights into how terrorists are using social media.

A new CVE strategy must do more to build and use the capacity of these partners to enable them to share the responsibility of diverting individuals from radicalisation.

Addressing the social and economic causes of violent extremism

There is no single pathway leading to radicalisation, as the process is unique to each person. However, there are some common social, personal and ideological drivers which assist the spread of violent extremism.

Commonwealth investment to build social cohesion, including in mental health, school participation, juvenile crime and unemployment, far outstrips that dedicated to CVE. The Government has committed approximately $545 million over four years as part of the 2014-15 Budget to promote social cohesion across multicultural communities.

While such initiatives deliver a public good in their own right, they can also help address many of the underlying factors that contribute to violent extremist tendencies.

Our broader social cohesion and social policy programmes, led by the Department of Social Services, should be more actively tailored to support CVE objectives. This could include:

- intelligence-led geographical prioritisation of programmes, resulting in better targeting of radicalisation hot-spots (suburbs, streets or organisations)
- integration of evaluation metrics into programme design, increasing our ability to understand the effectiveness of our CVE efforts.

Countering extremist narratives

Terror groups use highly targeted messages to appeal to vulnerable audiences. They rely on a range of humanitarian, ideological and identity-based narratives to gain support. They also use social media to great effect, while empowering supporters to independently generate and distribute propaganda. Young people don't necessarily receive information through traditional news channels, and are unlikely to trust government-led messaging. Yet Australia's online counter radicalisation efforts are still largely passive, based on government-badged information.

Community leaders and young Muslim Australians are often seen by at-risk communities as more legitimate, although some, particularly older individuals, lack the digital skills and media confidence necessary to engage online or in public debate. Governments should build the capacity of these credible voices in order to increase their reach and effectiveness. This may include funding for multimedia training and the development of online forums and videos.

For example, the UK currently employs film crews who work directly with community organisations to produce material which challenges extremist narratives. These crews work directly with community groups to ensure the end product maintains its identity (and therefore credibility). The material is distributed directly by these organisations, with only a small portion directly badged with government involvement.

Narratives: Which will an 18 year old choose?

Al-Qaeda-linked group Jabhat al-Nusra has posted videos of their fighters rescuing civilians from Assad regime snipers. The fighters look courageous and passionate.

Foreign fighters in Syria regularly post graphic images of dead children allegedly killed by the regime to highlight the humanitarian crisis.

ISIL releases recipes, such as pancakes, designed to feed jihadists after a hard day of fighting.

"Australia deplores the violence and suffering that is occurring in Syria, and Australian condemns all acts of violence against civilians, whoever is responsible.

The Government remains committed to a unified international response on Syria. Australia is continuing to work with like-minded countries to maintain pressure on the Syrian Government to end the violence and commit to an inclusive process of political transition.

The Australian Government is working with the United Nations and neutral non-government organisations to provide humanitarian assistance to the Syrian people. It has provided over $130 million in response to the Syrian conflict since it began in March 2011…"

Source: Australian Government Factsheet, 'Conflict in Syria: Australian Government's Position,' www.livingsafetogether.gov.au

Developing and delivering counter-narratives will be essential to reduce the pool of potential terrorists, but will need to be done in a way which manages the risks and challenges below:

Inadvertent affront – Messages need to be carefully developed in consultation with members of Australia's Islamic communities to avoid generating anti-government sentiment within the communities we are seeking to influence.

Community-led messaging – Partnering with communities does not mean they will agree with all aspects of government policy, and they may be open with their criticism. Additionally, close alignment with governments may compromise the credibility of community messengers.

Running a dynamic counter narrative – to effectively engage in real time debate, those delivering counter-narratives need to be agile and independent. This is generally at odds with existing bureaucratic risk management frameworks.

Deconfliction – the Government will need to ensure any counter-narrative work does not impact on law enforcement and security operations.

Accessing the necessary skills – Government does not currently have the social media, religious and other expertise necessary to effectively reach target audiences. Some of this capability can be outsourced, depending on the nature of the work and its sensitivity.

The Review recommends that the Commonwealth actively challenge extremist propaganda. This should be a priority under a new CVE strategy, and will require investment in capability to:

- monitor and increase our understanding of extremist narratives
- develop counter-narratives, including market research to gauge their effectiveness
- build the capacity of partners to deliver counter-narratives, such as through multimedia support, funding and training.

Managing returning foreign fighters

The flow of foreign fighters back to Australia is a long term challenge for governments. Returned fighters normally have the skills and capability to carry out terrorist attacks and past experience suggests that some are likely to be motivated to do so. Managing their return will be crucial in reducing the pool of potential terrorists in Australia long term.

The Government is currently investigating approximately 230 Australians who are either fighting for or supporting extremist groups – around 90 are currently in Syria, Iraq and the region and over 140 are here in Australia. While approximately 20 Australians are reported to have been killed in conflict zones, over 30 have returned to Australia from conflict zones. As the conflicts continue, the number of Australian foreign fighters looking to return to Australia will increase, which consequently increases the threat posed by foreign fighters to the Australian community.

To date, the primary focus of work associated with countering the threat of foreign fighters has been on disruption – preventing people from travelling to fight or facilitate in offshore conflict zones. A strategy for managing the return of foreign fighters is necessary so the Government can control the manner in which foreign fighters are permitted to return and impose stringent, individually-tailored conditions on returnees.

Return should be on the Government's terms and the strategy should provide a mechanism for setting those terms and conditions.

Options should include prosecution, revocation of citizenship, temporary or permanent exclusion from Australia while negotiated returns take place, mandatory de-radicalisation, cooperation with law enforcement and intelligence agencies, and rehabilitation support. The options should not be mutually exclusive – a range of options may be imposed on an individual, informed by an assessment of the level of threat the individual poses, coupled with an assessment of the needs of the individual to enable successful rehabilitation.

Recommendation

3. The Government significantly boost Counter Violent Extremism (CVE) activities:
   a. seek COAG agreement to a new national CVE strategy for endorsement in 2015, increasing Australia's national commitment to this work
   b. the Attorney-General bring forward a proposal as part of this effort with options to:
      i. establish and expand community and public-private partnerships to better reach at-risk or radicalised individuals
      ii. expand Commonwealth efforts to address the causes of violent extremism in Australia.
   c. the Attorney-General lead development of a proposal to counter the reach of extremist narratives in Australia.
4. The Attorney-General's Department coordinate across government to develop a strategy for managing the controlled return of Australian foreign fighters, subject to the Government's imposition of stringent, individually-tailored terms and conditions on returnees.

Six: Resourcing pressures

Key points

National security agencies cannot meet the ongoing requirements of the Efficiency Dividend without reducing core operational capabilities.

The Review recommends select national security agencies (ACBPS, AFP, ASIO, and ASIS) be either treated in the same way as Defence, with their operations exempt from the ED, or to be subject to a lower rate.

The Review concludes that select small agencies (ONA and OIGIS) face particular challenges, and so should be exempted in full.

Responding to the growing number of national security threats, such as terrorism, is straining national security resources.

The Review was tasked to consider the effect of the ED on the funding of national security agencies, in particular the impact on ACBPS[6], AFP, ASIO, ASIS, and ONA. The Review was directed to consider whether arrangements similar to those applying to Defence should be applied to these agencies.

The Review also included the Office of the Inspector General of Intelligence and Security (OIGIS) in its consideration, given its critical role in overseeing intelligence agencies' funding.

The recent decision to provide national security agencies with $632 million from 2014-15 to 2017-18 will significantly increase capacity to address CT priorities. However, national security agencies remain concerned that over time, their capability will continue to be eroded by the Efficiency Dividend (ED).

The Review has concluded that the agencies considered should not be fully subject to the ED, as these agencies are:

- primarily funded for operational activities, yet unlike other agencies with operational activities such as Defence their funding is treated as if it were for administration
- less able to produce efficiencies due to unique security-related expenses and administrative requirements.

In place of the full ED, national security agencies should have either a full exemption or a reduced rate of the ED applied to their operational funding.

[6] On 1 July 2015, the functions of the DIBP and the ACBPS will be integrated into a new department. The Review considered the effect of the ED on the ACBPS but has not included DIBP, ACBPS-related costs, or future DIBP operational and ABF-related costs, in budget models.

Findings of the Parliamentary Joint Committee on Intelligence and Security (PJCIS)

The PJCIS September 2014 *Review of Administration and Expenditure: No. 11 and No. 12 — Australian Intelligence Agencies* noted that 'while [ASIO, ASIS and ONA] are prudently implementing savings measures to absorb the impact of the efficiency dividend and other reductions in revenue, it is clear to the Committee that agencies are either reaching or have reached the point where they may no longer be able to address national security priorities if current funding patterns continue'.

The PJCIS also noted that '[it] has sufficient evidence before it to demonstrate that the continued implementation of the efficiency dividend and other savings measures will affect operations. The Committee views the risks associated with reducing an agency's operational capacity or capability as akin to the risks associated with reducing Australia's Defence capability'. PJCIS did not examine the operations and funding of the ACBPS, AFP or OIGIS.

National security funding

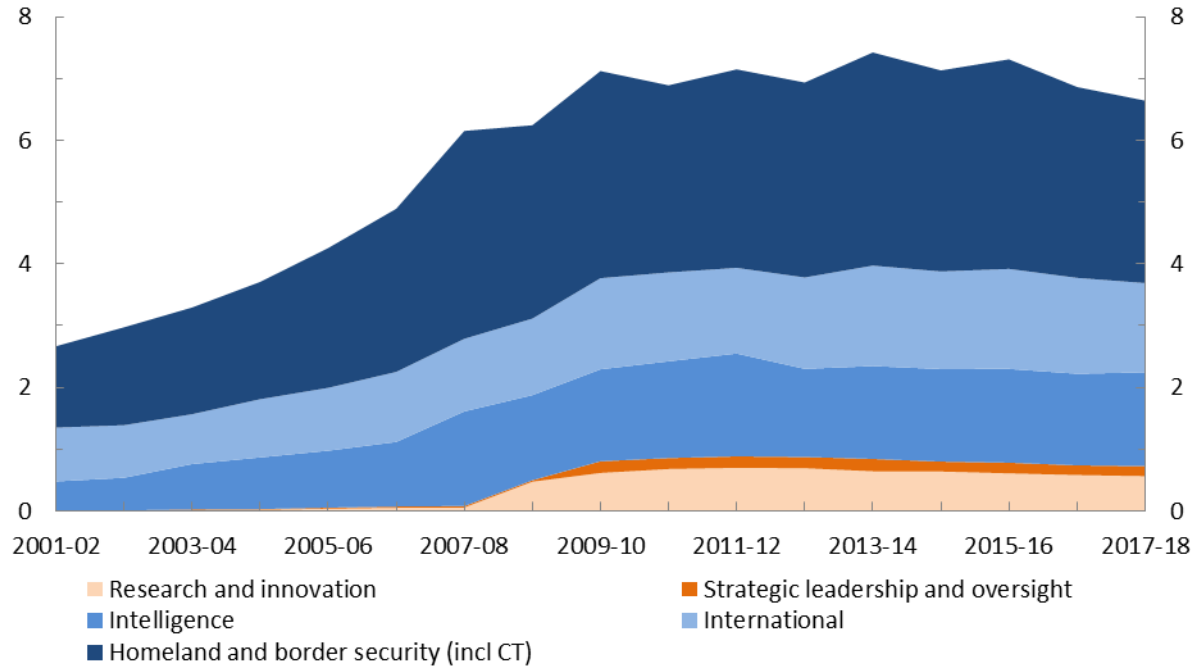
Key non-Defence national security agencies received substantial increases to base funding from 2001-02 to 2009-10. They also received significant temporary increases in funding to address specific emerging priorities, such as CT and people smuggling.

Funding for all national security activities plateaued after 2009-10. As demonstrated by Chart 12, it is projected to decline from 2014-15 to 2017-18 by around seven per cent in nominal terms, despite the recent decision to provide $632 million for CT measures from 2014-15 to 2017-18.

For the national security agencies that are the focus of this Review funding decreases by around 10 per cent from 2014-15 to 2017-18 in nominal terms. Half of this reduction is due to the ED, with the remainder due to terminating measures.

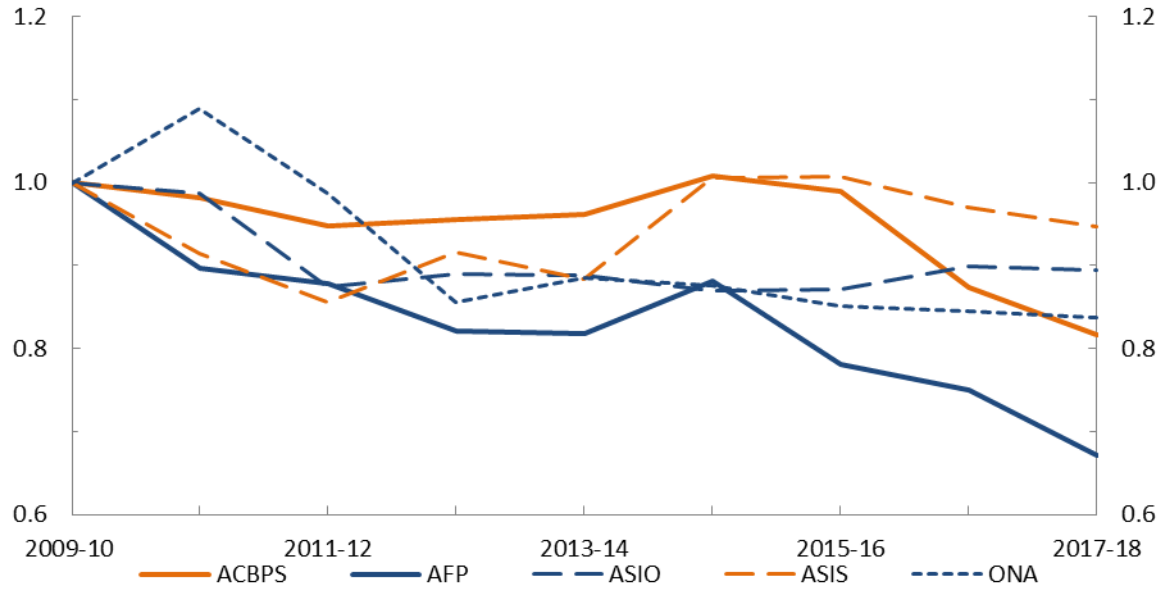
Chart 13 demonstrates the relative changes in the real value of Government funding provided to these agencies. For all agencies, the real funding available to them continues to decrease from 2014-15 to 2017-18.

Chart 12: Spending on non-Defence national security by activity, $ billion, nominal



Source: Department of Finance

Chart 13: Real Government funding for national security agencies, 2009-10 = 1.0



Should the ED apply to national security agencies?

The ED was initially introduced in 1987-88 to 'reduce the real level of resources directed to administer existing activities'.[7] This characterisation recognised the distinction between resources for *activities* and resources to *administer* those same activities.

The primary benefit of the ED is that it requires agencies and departments to generate savings without the Government having to individually identify them.

Ministers have the ability to redistribute the impact of the ED, within and between agencies in their portfolio, to redirect funding for priority activities. However, redistribution between agencies within a portfolio has been a rare occurrence: it has only been used twice in the 27 years since the ED was introduced, and not by these national security agencies.

Finding efficiencies to offset the ED is a challenge for all agencies. However, national security agencies have particular characteristics and constraints that make it difficult to achieve administrative efficiencies without ceasing activities.

National security agencies face an ED on both administration and activities

The distinction between resources for *activities* and resources to *administer* activities is usually established through the use of administered appropriations and departmental appropriations respectively. For example, welfare payments are funded by administered appropriations, and the staff necessary to make welfare payments are funded by departmental appropriations.

There are some agencies where both the activities and administration of those activities are funded entirely via departmental appropriations. Normal application of the ED to these agencies therefore goes beyond just administration. For this reason, a number of agencies have a full or partial exemption from the annual ED. This includes:

- Defence receives an 89 per cent exemption
  - The Defence Intelligence Agencies (AGO, ASD, and the Defence Intelligence Organisation) are largely exempt from ED as they are covered by the Defence operational capability exemption.

7 R Hawke, 'Ministerial statement: reform of the Australian Public Service', House of Representatives, Debates, 25 September 1986, p. 1450.

Alternative efficiency measures

Agencies exempt from the ED are often instead subject to direct efficiency studies, such as the recent Strategic Reform Program for Defence and the Efficiency Study of the ABC and SBS.

The Defence Strategic Reform Program allows for any savings identified to be reinvested into Defence's capabilities and supporting infrastructure. The ABC and SBS Efficiency Study recommended the efficiencies identified be returned to Government; for the ABC and SBS, this amounted to a savings package of $308 million over five years, or 4.4 per cent of their funding.

- the Australian Institute of Marine Science receives an 88 per cent exemption
- the Australian Nuclear Science and Technology Organisation receives an 85 per cent exemption
- the Commonwealth Scientific and Industrial Research Organisation receives a 70 per cent exemption
- the Australian Broadcasting Corporation (ABC) and the Special Broadcasting Service Corporation (SBS) receive a complete exemption

The scale of the exemption granted is equal to the portion of agency funding which is used for activities instead of administration.

AFP, ASIO, and ASIS do not receive any exemption from the ED, despite large proportions of their funding being devoted to activities. The ACBPS receives an exemption for two specific activities: the coast watch contractual arrangements and costs associated with processing inward cargo, including related intelligence and inspection functions (this eventuated from treating the Import Processing Charge as cost recovery). Otherwise, the remaining components of ACBPS are subject to the ED.

National security agencies are particularly constrained in finding efficiencies

The requirement to protect information, operations and people creates several points of unique inflexibility for national security agencies. This limits potential efficiencies. In particular, maintaining secure facilities and technology is expensive, limiting opportunities for relocation, co-location or outsourcing.

Much of the national security effort involves long term investment in partnerships, operations or capabilities. Capability, once turned off, cannot quickly be turned back on.

For example, the constraints associated with recruiting and training national security staff binds agencies to long term staffing plans. All staff must obtain and maintain high-level security clearances. Staff must develop highly specialised and unique skills (for some agencies it is up to six years before particular officers are fully effective in their roles).

The scope and complexity of successful national security activities are also increasing. Our adversaries' technical capabilities are growing at an exponential rate. Following a series of well-publicised leaks, they know more about our capabilities and techniques than ever before. That in turn has made it more expensive and difficult for national security agencies to keep up with or get ahead of them.

Small agencies are especially affected by the ED

While national security agencies have specialised or even unique administrative overheads that limit the capacity to find efficiencies, agencies such as the ACBPS, AFP, ASIO and ASIS have received substantial funding increases to do significantly more work over the past decade. This has eased their funding situation. The relatively large size of these agencies also gives them greater potential to identify savings, particularly compared to small agencies such as ONA.

Meeting the requirements of the ED is particularly challenging for small national security agencies, such as ONA and OIGIS. They have not received an increase in their funding, commensurate with that received by ACBPS, AFP, ASIO and ASIS and do not have the ability to continue to find efficiencies because of their small size and the national security restraints under which they operate.

Case Study: Impact of the ED on ONA

To meet ED-driven savings targets, in 2013 ONA did not replace the retiring Russia analyst, leaving just one analyst to cover Russia, the former Soviet States and Western Europe at a time of burgeoning demand for analysis of this part of the world.

ONA has also had to reduce open source resources to protect other assessment priorities at a time when social media exploitation is becoming a more important feature of law enforcement and intelligence efforts.

Impact of the ED on national security agencies

National security agencies have identified specific actions they would need to take to meet the ED over the forward estimates.

- The AFP will reduce by 451 staff (seven per cent) from 2014-15 to 2017-18. This will impact on all areas of the AFP including protection response, intelligence support, and serious and organised crime.
- The ACBPS will reduce by 231 staff from 2014-15 to 2018-19. In the past the ACBPS has targeted operational ED savings on non-frontline areas. Restricting savings to these areas will not be possible in the future.
- ASIO will tightly prioritise resources on the high end of the threat spectrum, with less scope to address other threats or to identify emerging issues.
- ASIS will substantially reduce or abandon intelligence collection on a range of enduring issues of importance to Australia (other than CT).
- ONA will reduce by seven staff from 2014-15 to 2016-17. This will weaken ONA's capability.

Agencies have identified the following risks to national security outcomes from continued reductions to base funding:

- decreased capability to address the National Intelligence Priorities and collection requirements
- less analytical support to inform government decision-making
- inadequate domestic coverage of national security threats, including on CT
- increased risk of gaps in national security activity, including at borders and in law-enforcement
- degrading domestic and international national security partnerships – less leverage, less intelligence
- a growing potential for missed opportunities as agencies prioritise the urgent or the highest priority at the expense of long-term priorities.

An argument in favour of maintaining existing arrangements is that it does impose discipline on the national security agencies. But this may be described as a 'grind them down, top them up' approach: the ED erodes capability until the resultant vulnerability is too large or too time sensitive to ignore, at which time budget supplementation must be sought.

Proposed approach

Having considered all of these factors, and consistent with the way in which the ED is applied to Defence, the Review recommends exempting the 'operations' of the five national security agencies from the ED.

The activities of these national security agencies are just as operational as those of Defence, as both undertake activities that contribute to national security. Both Defence and national security agencies have:

- areas that directly undertake action, at times at extreme personal risk, such as containing imminent violent threats, enhancing Australia's response to

emerging crises, and securing critical outcomes in Australia's interest

- areas and structures that provide direct support to operations, including intelligence collection and analysis, training, high-tech operational capabilities and forensics
- areas and structures that provide indirect support operations, including back-office administration.

Defining the 'operations' of national security agencies

The Review considers that an appropriate definition of the operations of national security agencies would be:

- any collection, assessment or activity that is directly linked to one or more of the Government's national security priorities
- an activity prescribed by relevant legislation (such as the Intelligence Services Act 2001)
- any activity that is directly supporting the two categories above.

The ED would continue to apply to the non-operational or administrative activities of these agencies. The exemption would apply to existing funding and any new funding sought via NPPs.

Exempting operations from the ED would avoid the budget-driven erosion of national security capabilities. National security agencies' base funding would be assured, providing a firmer foundation for delivering long-term outcomes.

The Review concluded it would not be possible to distinguish between non-national security operations and national security operations of agencies for the purpose of applying any exemption to one but not the other. Furthermore, the operational support capabilities often underpin both non-national security and national security operations (such as police forensics and surveillance).

Small agencies

ONA does not have the same scale of operational activity as ACBPS, AFP, ASIO and ASIS, and OIGIS has no operational activity. However, they do play a crucial part in the proper operation of Australia's national security machinery, and, as outlined above, are still subject to the same constraints on finding efficiencies due to the nature of their work but without a sufficient funding base from which to absorb the ED's required savings.

Ongoing efficiencies

The Review notes that the ED will continue to drive the identification of efficiencies in administrative functions of the ACBPS, AFP, ASIO and ASIS. These agencies will still be required to seek value for money in their operations, and, continue to find efficiencies where possible.

The Review recommends national security agencies continue to be subject to efficiency processes such as the Functional and Efficiency reviews being conducted by the Government.

Implementation

In conclusion, the Review recommends that the ED be removed from the operational activities of the ACBPS, AFP, ASIO and ASIS, and for the ED to be completely removed from ONA and OIGIS. This approach would require a process to agree to the quantum of relevant agency budgets which may receive an ED exemption.

All exemptions should start from 2015-16 in order to allow sufficient time to implement the proposed changes.

For AFP, ASIO and ASIS this would have an estimated cost of $180 million from 2014-15 to 2017-18, and an ongoing annual cost of at least $90 million each year thereafter. It is unlikely that offsetting savings could be identified elsewhere.

The cost for the ACBPS (to be incorporated in the new DIBP incorporating ABF) is unable to be accurately estimated at this time. Based on in-principle support by NSC for this decision to apply to the ACBPS and the relevant functions of the new DIBP and ABF, costs would then be calculated and provided to the Department of Finance for approval. Were the same methodology applied to the existing ACBPS, the exemption would cost $80 million from 2014-15 to 2017-18 with an ongoing annual cost of at least $40 million thereafter.

(a) Exempting activities of AFP, ASIO, ASIS from the ED: Indicative fiscal impact ($m)			
'14-15	'15-16	'16-17	'17-18
-	*-30*	*-70*	*-80*

Does not include impact for ACBPS/reformed DIBP.

This full exemption of ONA and OIGIS from the ED would have an estimated cost of $5 million from 2014-15 to 2017-18, and an ongoing annual cost of at least $3 million each year thereafter.

(b) Removing the ED from ONA and OIGIS: Indicative fiscal impact ($m)			
'14-15	'15-16	'16-17	'17-18
-	*-1*	*-2*	*-2*

Alternative approach

A lower cost option would be to apply the ED at a lower rate to agency operations, set at 0.5 per cent.

This would continue to drive some efficiencies in the operations of national security agencies, and partially mitigate the identified risks to the national security capability. A reduced ED of 0.5 per cent for national security operations in addition to the full ED for these agencies' administration, would ensure there is a degree of discipline maintained on national security agency spending on operations.

This approach would also apply the reduced ED of 0.5 per cent to the whole of ONA and OIGIS. It would need to resolve the same implementation issues identified above.

(e) Apply an ED of 0.5 per cent to agency operations: Indicative fiscal impact ($m)			
'14-15	'15-16	'16-17	'17-18
-	*-20*	*-50*	*-50*

Does not include impact for ACBPS/reformed DIBP.

Introducing a reduced rate of ED would have an estimated cost of $120 million from 2014-15 to 2017-18, and an ongoing annual cost of at least $60 million each year thereafter.

Recommendation

5. The Government adjust its approach to seeking efficiencies from the national security agencies by:
   a. from 2015-16, removing the efficiency dividend (ED) from all of the ASIO, ASIS, and AFP operations
   b. from 2015-16, ending the application of the ED to the ONA and the OIGIS
   c. in-principle, from 2015-16, removing the ED from all ACBPS operations that will transition to the new DIBP including the Australian Border Force with final costs to be agreed with the Department of Finance and a detailed proposal brought to NSC by 30 June 2015
   d. noting that the AFP, ASIO, ASIS, DIBP and ONA would be subject to the ongoing whole-of-government non-ED efficiency processes, including the functional and efficiency reviews, including the Efficiency through Contestability Programme.

   Alternatively:

   e. from 2015-16 applying a 0.5 per cent ED to ASIO, ASIS and AFP operations, to all ONA and OIGIS funding, and in-principle applying a 0.5 per cent ED to all ACBPS operations that will transition to the new DIBP with final costs to be agreed with the Department of Finance and a detailed proposal brought to NSC by 30 June 2015.

Seven: National terrorism advisories

Key points

The current terrorism alert system, with separate classified and public levels, is unnecessarily complex, both for the public and officials.

Additionally, there are not enough public alert levels, making it difficult to raise and lower the alert level in response to a temporarily increased threat environment.

As the terrorist threat dominates the media, there is a public expectation that the Government will provide useful information on terrorist threats and advice about required changes to behaviour.

On 12 September 2014, the National Terrorist Public Alert Level was raised from Medium to High. This was the first change to the alert level in 12 years. While the change drew interest, there was limited public advice about what it meant.

The Review recommends the National Threat Level (Threat Level) for terrorism issued by the DG of Security be publicly announced with an unclassified narrative. This would render the existing National Terrorist Public Alert System (Public Alert System) redundant.

Background

In 2003, Australia introduced the Public Alert System to provide coordinated public information about the risk of a terrorist attack in Australia through a Public Alert Level (Alert Level). The Alert Level can be applied Australia-wide or to specific states and territories, business/industry sectors or geographic locations. The intended audience is the general public, businesses and critical infrastructure owners/operators.

There are four public alert levels:

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

The Alert Level is informed, but not determined, by the classified Threat Level set by the DG of Security. The Threat Level reflects ongoing assessments by ASIO's National Threat Assessment Centre.

The Threat Level and the Alert Level convey different information. The Threat Level reflects the current assessed threat of terrorism to Australia and its interests, while the Alert Level is intended to advise the public about the severity of the terrorist threat and how they should prepare.

While the Threat Level is classified, it was publicly referenced as part of the justification for raising the Alert Level on 12 September 2014.

Use of the Public Alert System

The process to change the Alert Level involves consultation between the Commonwealth and the states and territories. However, the decision is made by NSC or the Prime Minister based on advice. In 2014, the Secretary of PM&C advised the Prime Minister to change the Alert Level.

The process to raise the Alert Level in September 2014 worked well and all key decision making points were used. This included direct discussions between the Prime Minister and Premiers and Chief Ministers before the Alert Level was raised.

ANZCTC review of the Public Alert System

In May 2012, the ANZCTC established the Alert System Working Group (ASWG) to report on the effectiveness of the Public Alert System. While the ANZCTC agreed in-principle to the ASWG's recommendations, momentum was lost during the 2013 election period.

In its report the ASWG:

- noted decision makers did not clearly understand the differences between the public alert system and the classified threat level
- believed the public messages did not meaningfully describe the different Alert Levels
  - This could lead the public to expect that a changed level would inform or trigger an operational response by state and territory law enforcement agencies.
- recommended the Alert Levels be replaced with tailored public advisory messages designed to explain, reassure and influence behaviour
- noted an alternative was to maintain the current system but include more detail in the National Counter-Terrorism Handbook on the intent of the system and thresholds for changing the Public Alert Level.

Alternative Australian model

The Review has concluded that:

- having two systems in place is unnecessarily complex, both for the public and for many officials
- there is not enough flexibility or precision in the definition of the levels, making it difficult to raise and lower the Alert Level in response to a temporarily increased threat environment
- as the terrorist threat dominates the media, there is a public expectation that Government will provide better information on terrorist threats
- effective public communications should contain useful advice about required changes to behaviour.

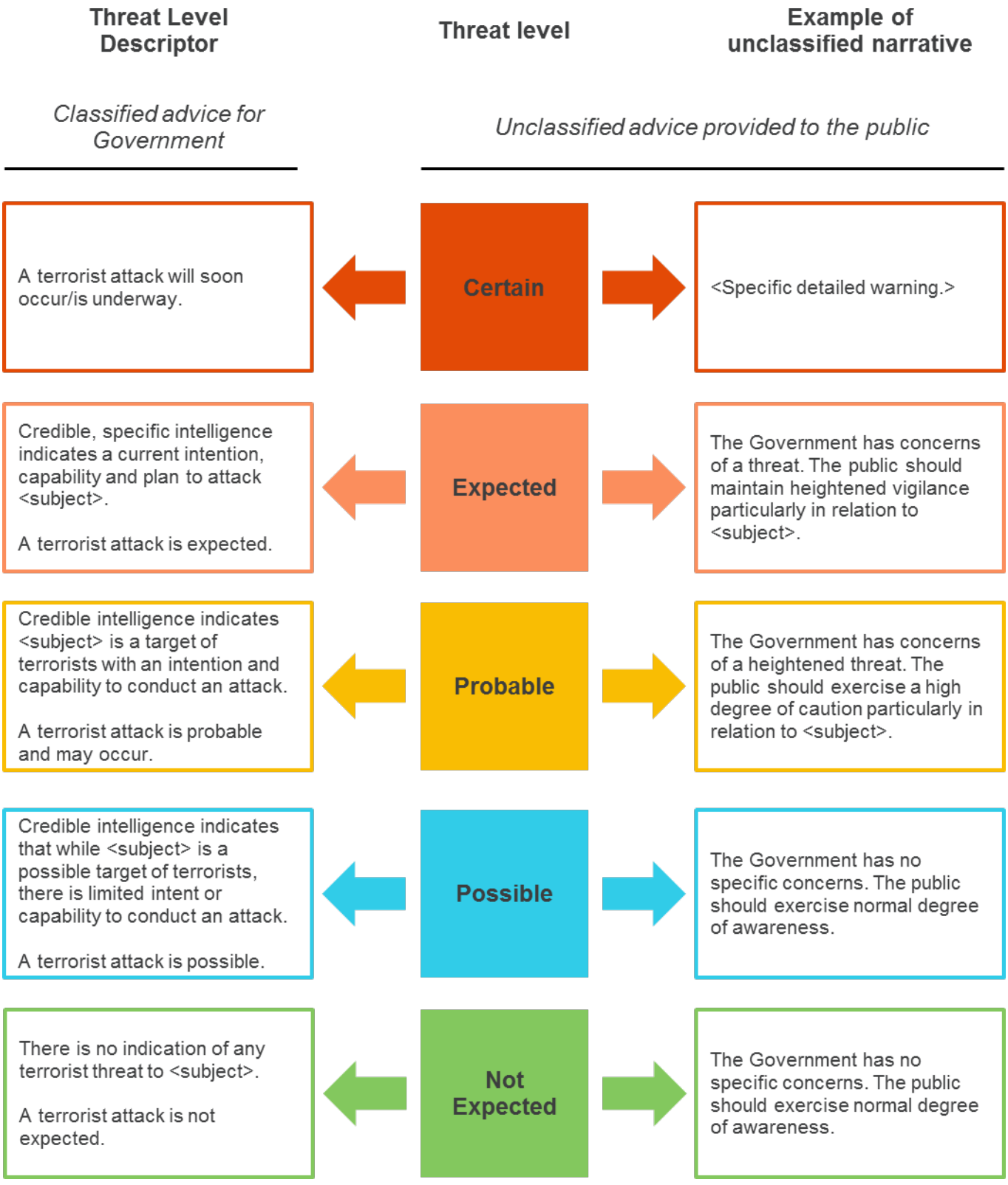
Based on these conclusions, the Review proposes that the Threat Level be made public and accompanied by an unclassified narrative.

The public alert system would no longer be required. This means there would only be one system in place.

Under this system, the Threat Level would be public. To be more explicit about the implications of the threat, there would be some minor changes to threat level descriptions. All other existing ASIO threat assessments and all supporting intelligence would remain classified.

The DG of Security would continue to set the national Threat Level and would inform the Prime Minister of the reasons for any change. This would allow the Prime Minister time to engage with Premiers and Chief Ministers. In deciding to raise the Threat Level, ASIO would continue to consult with states and territories at the working-level. The DG of Security would also issue a public narrative.

Chart 14: New model descriptors and example advisories



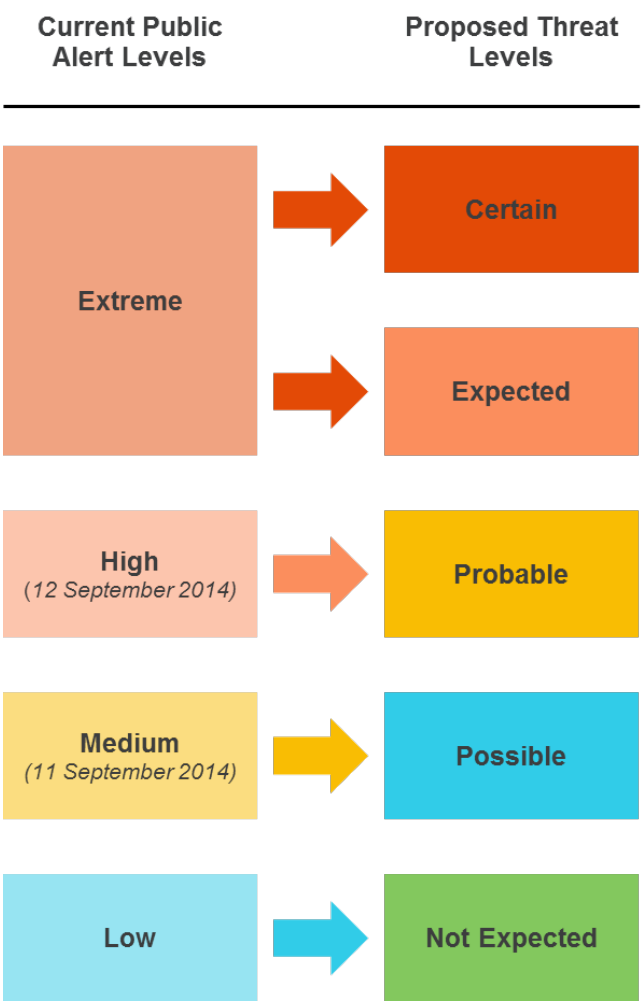
By being more explicit about the Threat Level and the accompanying narrative there would be minimal disruption to those businesses that have built their contingency plans on the basis of the current Public Alert Levels.

A single public Threat Level for terrorism and an accompanying unclassified narrative has many benefits.

- The proposed model rebalances the threat levels to reflect the new 'normal' environment as well as giving one extra public level at the higher end of the spectrum.
- It would replace two alert systems with one single system. Under this model, the DG of Security would be ultimately responsible for setting the Threat Level and issuing public narratives.
- The narratives would provide relevant information that could be updated to reflect different circumstances without changing the threat level.
- Specific sectoral information could be included in the narratives as needed.

In designing a streamlined system, we have consulted closely with states and territories. Their reaction has been uniformly positive. They have confirmed that they would welcome a referral of the proposed model to the ANZCTC for their consideration and, if agreed, adoption.

Chart 15: Concordance table



Recommendation

6. The Attorney-General refer the modified national threat advisory system to the ANZCTC for consideration.

The following charts illustrate the differences between the current and streamlined public advisories:

Chart 16: Current model – National Terrorism Public Alert System

Public Alert Level	Alert level description (*as listed on national security websites*)
Medium *11 September 2014*	A terrorist attack could occur.

On 12 September, the Public Alert Level was raised from Medium to High

High *12 September 2014*	A terrorist attack is likely.

Chart 17: Proposed Model – Threat Level

Threat Level	Example of unclassified public narrative
Possible *11 September 2014*	The Government has no specific concerns. The public should exercise normal degree of awareness. If you see anything suspicious, report it to the **National Security Hotline 1800 1234 00**.

With the proposed changes to the threat level system, the Threat Level would have been raised from Possible to Probable, and the following public advisory would have been issued.

Probable *12 September 2014*	The Government's threat concern is heightened. This is not based on knowledge of a specific attack plan but rather a body of evidence that points to the increased likelihood of a terrorist attack in Australia. Security and intelligence agencies are concerned about the increasing number of Australians working with, connected to, or inspired by terrorist groups such as ISIL, Jabhat Al-Nusrah, and al-Qa'ida. Raising the alert level to Probable is designed to increase vigilance and raise awareness in the community. While it is important the public are aware of the increased threat, Australians should continue to go about their lives. Strong arrangements are in place to detect, prevent and respond to terrorism. Owners and operators of critical infrastructure and places of mass gathering and encouraged to review their security plans and update their contact details with their State or Territory police counter-terrorism unit. If you see anything suspicious report it to the **National Security Hotline 1800 1234 00**.

Annex: Abbreviations

ABC	Australian Broadcasting Corporation
ABF	Australian Border Force
ACBPS	Australian Customs and Border Protection Service
ACC	Australian Crime Commission
ACTC	Australian Counter-Terrorism Centre
ADF	Australian Defence Force
AFP	Australian Federal Police
AGD	Attorney-General's Department
AGO	Australian Geospatial-Intelligence Organisation
Alert Level	Public Alert Level
AMSA	Australian Maritime Safety Authority
ANZCTC	Australia-New Zealand Counter-Terrorism Committee
AQ	al-Qa'ida
AQAP	al-Qa'ida in the Arabian Peninsula
AQIM	al-Qa'ida in the Islamic Maghreb
ASD	Australian Signals Directorate (formerly Defence Signals Directorate)
ASIO	Australian Security Intelligence Organisation
ASIS	Australian Secret Intelligence Service
ASWG	Alert System Working Group
AUSTRAC	Australian Transaction Reports and Analysis Centre
BLU	Business Liaison Unit
CDPP	Commonwealth Department of Public Prosecutions
COAG	Council of Australian Governments
CT	counter-terrorism
CT Coordinator	Counter-Terrorism Coordinator
CVE	countering violent extremism
Defence	Department of Defence
DG	Director-General
DHS	Department of Human Services
DIBP	Department of Immigration and Border Protection
DIO	Defence Intelligence Organisation
DSS	Department of Social Services
ED	Efficiency Dividend
Education	Department of Education
Executive Group	Senior Executive Counter-Terrorism Group
INSLM	Independent National Security Legislation Monitor
JCTT	Joint Counter-Terrorism Team
NCTC	National Counter-Terrorism Committee
NSC	National Security Committee of Cabinet
NTAC	National Threat Assessment Centre
OIGIS	Office of the Inspector General of Intelligence and Security
ONA	Office of National Assessments
OSB	Operation Sovereign Borders
OTS	Office of Transport Security
PJCIS	Parliamentary Joint Committee on Intelligence and Security
PM&C	Department of the Prime Minister and Cabinet
Public Alert System	National Terrorist Public Alert System
SBS	Special Broadcasting Service Corporation
Threat Level	National Threat Level
UK	United Kingdom
UPS	United Postal Service
US	United States

Photo Reference

Front cover images

From left to right

Hacker at work	iStock
QLD police	iStock
Man in mask with gun	iStock
Australian flag	iStock

Internal images

Page 38	Pancakes	2007 Uyen Le