Australian National University

National Security College

POLICY OPTIONS PAPER
No 4, August 2017

Federating security

Anthony Bergin

Key points

- National security has too often been run as a 'top-down' policy, with a tendency towards a 'Canberra knows best' approach.
- The states and territories contribute many of the powers and capabilities needed to support our overall effort in dealing with a wide range of national security issues.
- Harnessing all jurisdictions for national security purposes will be essential to address our national security challenges and their role here will only grow.

Policy recommendations:

- COAG should commission a fundamental study to examine how the states and territories operate in the area of national security.
- The Department of Prime Minister and Cabinet, with First Ministers' departments, should convene a regular summit on national security issues for senior officials and key senior ministerial advisors.
- The new Home Affairs portfolio should establish better practical coordination and information sharing across jurisdictions as an ongoing priority.

Canberra doesn't own national security

In our federal system of government, there is always a tension between decision-making at different levels of government. National security has very often been run as a 'top-down' policy, in part because security policy has traditionally focused on defence, foreign affairs and intelligence. These are all primarily Commonwealth responsibilities.

However, the 'Canberra knows best' approach does not work across the full range of national security issues. Commonwealth-States interactions can be a critical 'rub point' in achieving day-to-day security.

As the Commonwealth shakes up its security arrangements with a Home Affairs ministry, it provides an opportunity to better integrate the roles of the jurisdictions: they contribute many of the powers and capabilities needed to support our overall effort in dealing with a wide range of national security issues.

The Australian public expects that at the States and territory level, (and sometimes at the local level),[1] their governments will work with the Commonwealth to provide the necessary degree of security to allow their way of life to continue as normal. National security is an increasing concern of States agencies with a broad range of service delivery, policy, and regulatory functions which could be jeopardised by a range of hazards.

Cooperation remains difficult

States and territory representatives join together through the Australia-New Zealand Counter-Terrorism Committee (ANZCTC) and First Ministers through the Council of Australian Governments (COAG).

But cooperation between the jurisdictions and the Commonwealth often remains a challenge. Different States come at the issues from different angles as they have different responsibilities: communications between States and federal entities on national security can be difficult.

This also leads to practical problems. The AFP, for example, can only investigate crimes under Commonwealth laws, and apart from terrorism, there aren't that many of those: the vast majority of crime is a States law matter.

The main challenges are the legislative impediments for sharing intelligence with non-law enforcement agencies, and the capacity of law enforcement officers to use nationally classified material in court proceedings. The sharing problem increasingly relates to cultural issues: 'not sharing with the Feds' or 'knowledge is power' cultures. But the momentum from the creation of a Home Affairs ministry should strengthen Commonwealth-States information sharing around criminal intelligence.[2]

A joint approach is needed

There's scope to strengthen a more whole-of-nation approach to security that reflects the current range of security priorities across our federation. But the States aren't always in a position to identify and distil common security interests amongst themselves and clarify joint policy positions to bring them to COAG.

We should develop an approach whereby States agencies benefit from access to each other's skills, experience and capabilities across many security issues: the jurisdictions are first responders for a range of incidents, such as counterterrorism, emergency management and critical infrastructure protection.

States' roles in national security

There are a range of areas where the States have a key role in national security, notably counter-terrorism, (Joint Counter-Terrorism Teams consist of States police, AFP and ASIO), critical infrastructure protection (the States own, operate, or license most critical infrastructure) and natural disaster response.

Other areas would include port security, organised crime and illicit drugs, protecting crowded places and public health preparedness. A key area that has attracted considerable controversy, especially with the sale of States electricity poles and wires, is asset recycling: balancing asset sales and other forms of foreign involvement with national security imperatives.

But two issues are of growing importance: cyber security and countering violent extremism.

Cyber security

The 2016 Commonwealth Cyber Security Strategy sets out a devolved approach. The Australian Signals Directorate (ASD), soon to become a statutory authority, has capability and knowledge in this field. It advises on standards in the Information Security Manual and passively monitors for compromise and post compromise response. ASD offers the jurisdictions generic advice, but the States are responsible for their own cyber security.

NSW and South Australia, for example, now have their own Chief Information Security Officers who sit in their Premier's Department. Victoria is appointing one. But they have few resources or staff. South Australia and Queensland are in some ways leaders. South Australia has convened two cyber forums and Queensland has established a Cyber Security Unit.

Generally the States have been more concerned with 'information security' in compliance with International Standards Organisation standards, Audit Office recommendations and federal legal policy settings, such as the Privacy Act and the Protective Security Policy Framework. States

audit offices been active in reviewing the compliance of States agencies with ASD guidelines against cyber security attacks.

But there has been little evidence of active, external-facing cyber security engagement, education, or enforcement from States governments, or the creation of 'cyber units' in States enforcement bodies. States governments need to embed cyber security within their organisations and processes. But the jurisdictions have largely conceptualised cyber security as a federal responsibility, involving cyber threat intelligence and information sharing and look to the federal government to provide more hands-on solutions.[3]

It would be naive to assume that States governments have not been subject to foreign interference in the same way as Commonwealth agencies. This is of particular interest where there is a nexus between federal and States governments in sensitive areas and capabilities, such as counter-terrorism.

To date, however, we haven't adopted a truly national view of network failures. ASD, for example, has appeared to adopt a conservative approach the active defence and monitoring of systems, and providing response to the States' cyber networks.

There would be some appetite by the States for the federal government to undertake these roles, possibly on a fee for service basis. Alternatively ASD could perform at least some of these roles, (network providers have a big role to play), with appropriate resourcing. The Commonwealth could second cyber security experts to the smaller States. But while the States may not want to, they need to build up their own capability.

As States governments are vulnerable to malicious cyber activity, there's urgent work to be done to strengthen how the States would cooperate in the event of major cyber disruptions. The States will be the first responders to infrastructure network disruptions, although this is complicated by critical infrastructure being split between public and private operators.

Expanding the cyber incident exercises program to include the States would be helpful, and there are some federal resources being committed to this end.

An additional challenge for the States is how they work together to integrate public and private sector information through the new Joint Cyber Security Centres (JCSCs) in key capital cities. In theory, the JCSCs could become coordinated incident response centres and draw in private sector representatives from critical infrastructure sectors, as well as federal cyber experts.

The recent announcement that the Special Adviser to the Prime Minister on Cyber Security will head the Australian Cyber Security Centre (ACSC) should advance a whole of economy shared solutions approach. This should improve the chances that the JCSCs in the States respond to industry concerns that the federal government is not sharing back.

Countering violent extremism

There's a national CVE policy, with an intervention framework to help people move away from violent ideologies and a CVE Centre in the federal Attorney-General's department.[4] The ANZCTC, that reports to COAG, has a CVE Sub-Committee with States representatives, including from social policy agencies.

Under the Commonwealth's Living Safe Together program, the role of States is to tailor and deliver intervention activities and processes. The jurisdictions most affected (NSW and Victoria) have adopted a case management approach and have their own body of experts to draw upon to flexibly tailor interventions with local services of support. These may include religious and ideological mentoring, employment and educational support, family and relationship counselling and psychological or other clinical support. This supports the notion that CVE programs are not intelligence-gathering exercises.

In that sense, national CVE policy is not as 'top down' as it looks: it does recognise that the States have an essential role to play in CVE,

leveraging local networks. The Commonwealth is stronger in regional and international CVE engagement, (bringing back best practice information), and talking with technology companies on issues related to countering terrorism propaganda online. It's well placed to coordinate and fund CVE research and training and assessment tools.

Services may not necessarily be marketed under the banner of CVE, a brand that has been called into question by sections of the community. The States will be more effective in leading, with local communities responding better to broader social cohesion programs. The problems aren't necessarily the same in Melbourne as they are in Sydney, so a uniform approach won't work. But there's been very little cross jurisdictional information sharing on CVE best practices.

And while there are Joint Counter-Terrorism Teams in each jurisdiction, there is no equivalent in the CVE area that brings Commonwealth agencies like Heath, Social Services and Human Services into task force arrangements with the States.

The way ahead

Ministerial councils that assist COAG around national security, such as the Law, Crime and Community Safety Council, exist 'hand to mouth'; they don't function strategically.

COAG should consider federalism in the national security space and examine how to improve its role as a strategic forum on national security. A special annual COAG meeting on cyber security would be useful.

There's a need for a COAG study to examine how the States and territories operate in the area of national security, in the same way COAG did with regulation by commissioning the seminal Hilmer Review into national competition policy over 20 years ago.

This could be supported by a regular summit on national security issues for First Ministers' senior officials, other key States and territory ministerial senior staff advisors and senior federal security officers. There may also be value in a clearing house, so the jurisdictions can learn from the experience of other States in national security issues.

Endnotes

[1]Anthony Bergin 'Local government and Australian counter-terrorism strategy' *Journal of Policing, Intelligence and Counter Terrorism,* Volume 12, Issue 1, 2017
[2]John Coyne, 'Law enforcement and the Home Affairs portfolio' *The Strategist,* 20 July 2017
[3]In part this States' view has been driven by legacy classification and legality issues: ASD has great technical capability in what is now cyber security, that grew out of classified and illegal (for everyone other than ASD) activities.
[4]It is not yet clear whether the CVE Centre will move to the Home Affairs Ministry.

About this publication

This series of National Security College Policy Options Papers offers short, evidence-based and forward-looking insights for policy-makers on topical security, foreign affairs and geostrategic issues facing Australia domestically, in the Indo-Pacific region and globally. We seek contributions from and collaborations with qualified researchers and experts in these fields.

T +61 2 6125 1219
E national.security.college@anu.edu.au
W nsc.anu.edu.au

@NSC_ANU
National Security College

CRICOS Provider #00120C

About the author

Dr Anthony Bergin is a Senior Research Fellow at the ANU National Security College and a Senior Analyst at the Australian Strategic Policy Institute. He previously taught homeland security at the University of New South Wales at the Australian Defence Force Academy. His research is on Australian national security, maritime security and non-traditional security issues in the Indo-Pacific. He blogs at the Asia & the Pacific Policy Society's *Policy Forum* and ASPI's *The Strategist.*

MO_NSC16797