



Improving National Security Governance:

Options for Strengthening Cabinet Control and Parliamentary Oversight

Dr. William A. Stoltz

Key Points

- Following decades of investment, legislative reform, and structural adaptation to changing threats, Australia's national security apparatus is now one of the most complex and sophisticated in the world.
- Yet, the Parliamentary and ministerial structures for guiding Australia's national security institutions have evolved surprisingly little.
- The result is that Australia's Parliament and Cabinet face a number of limitations to scrutinising and guiding our security and intelligence organisations.
- This paper proposes reforms to bolster the capacity of our leaders to hold national security institutions accountable as Australia moves into an era of heightened strategic complexity and risk.

Key Recommendations

- An assistant or junior Minister for Intelligence should be appointed, with responsibilities to work across national security portfolios to support senior Cabinet ministers and the Prime Minister on matters relating to national security strategy, managing investment in intelligence capability and reforms to enabling legislation.
- The Parliamentary Joint Standing Committee on Intelligence and Security (PJCIS) should be empowered to commission the Inspector-General for Intelligence and Security (IGIS) to undertake reviews and investigations and the IGIS should be resourced accordingly. This will deepen oversight of Australia's expansive national security and intelligence ecosystem and improve Parliament's trust and understanding of operational agencies.
- The Independent National Security Legislation Monitor (INSLM) should become a full-time appointment and be resourced to provide regular support and advice to the PJCIS.
- At least one security-cleared adviser should be allocated to the office of PJCIS members to bolster their capacity to undertake committee business.
- National Intelligence Community (NIC) agencies should provide staff on secondment to bolster the work of the PJCIS Secretariat within the Department of the House of Representatives.

Improving the Executive's Strategic Control of Security and Intelligence

Australia's primary decision-making forum on intelligence and security is the National Security Committee of Cabinet (NSC), which has existed in various forms since the Fraser Government created the National and International Security Committee. Supported by a gallery of senior bureaucrats, today's ministerial membership of the NSC includes the Prime Minister, Deputy PM, the Treasurer and Finance Minister, the Foreign Minister, Defence Minister, Home Affairs Minister and Attorney-General.

While the intent of the NSC is for the executive to guide Australia's security policies in an informed, concerted fashion, the reality is that much of the enterprise and operational decision-making concerning Australia's intelligence and security is diffused across ministerial offices and an expanding community of agencies and departments with influence over intelligence resources and security.

Outside NSC meetings, the Treasurer and Finance Minister have great impact on Australia's immense national security budget, while the Attorney-General can exercise close influence over the legislative and oversight mechanisms affecting agencies' day-to-day operations. Concerning agencies' use of their often-extraordinary powers, the Defence Minister, Home Affairs Minister and Foreign Minister exercise great authority. This is particularly the case for the Home Affairs and Foreign Ministers who under law must sign-off on intelligence operations. Transcending all these decisions is the Prime Minister, who can exercise their imprimatur to shape any ministerial decisions.

This diffusion of executive decision-making outside of the NSC is in part a practical response to the proliferation of agencies and departments with national security and intelligence equities. In 2017 the Turnbull Government formed the National Intelligence Community (NIC) in recognition that the agencies at the core of Australia's intelligence enterprise had expanded from six traditional foreign and domestic collection and assessment agencies to include those with a focus on transnational, serious and organised crime, money-laundering and terrorism financing. The creation of the NIC was also accompanied by the creation of the Home Affairs Portfolio, which drew the Australian Border Force, Emergency Management Australia and relevant policy units from other departments into a new homeland security community led by the Department of Home Affairs.

So, if we include the behemoth Defence Portfolio alongside the NIC and Home Affairs Portfolio, since 2017 Australia's leaders have had to contend with three tribes representing similar and overlapping portions of the nation's security and intelligence enterprise

and totalling at least 16 agencies and departments. Considering that the NIC contains agencies that are also resident in the Defence (DIO, ASD, AGO) and Home Affairs (ASIO, ACIC, AFP, AUSTRAC) portfolios, the task of planning the capabilities and direction of Australia's security and intelligence enterprise has become a vexed and time-consuming one, even for the most capable Cabinet member.

New shocks and risks in Australia's strategic environment have broadened further still the scope of issues – and agencies – pertinent to Australia's security. The COVID-19 pandemic and emergent biosecurity threats, have made Australia's Health portfolio profoundly relevant to national security and intelligence planning. Next generation internet-connectivity and the urgent technological development needs of Australia's Pacific neighbours has reinforced the security role of Australia's communications, infrastructure, and industry departments. So too have concerns over foreign interference, social cohesion, and societal resilience brought departments of education and social services into the security domain.

Australia's leaders must now navigate a bureaucratic maze when it comes to deliberations on what intelligence capabilities to invest in and what legislative reforms to prioritise.

Critical intelligence capabilities, enabling services and relationships now intersect and stretch across the public service but with no single minister positioned to view and understand it all and help adjudicate between powerful, occasionally competing, public servants. Consider too that all of the senior ministers responsible for national security activities, including the PM, also have extensive responsibilities for other non-security aspects of government, so their attention can be greatly restricted.

Appointing an assistant or junior Minister for Intelligence could greatly improve the ability of Cabinet to exercise informed, strategic leadership over Australia's modern intelligence and security enterprise. Positioned under the PM, the remit of a Minister for Intelligence should not necessarily include exercising any of the existing operational authorities of senior national security ministers, like approving intelligence collection activities. Rather, their responsibility should be to advise NSC and senior ministers on strategic issues transcending Australia's intelligence and security enterprise, such as the preparation of agency

budgets, capability investments, and the consideration of legislative reforms affecting the powers and oversight of agencies.

It is necessary that a ministerial appointee perform this function, as opposed to a public servant like the Director-General National Intelligence or a National Security Adviser, because only a Minister for Intelligence under the PM would have the effective standing to gain access to the multitude of portfolios now comprising Australia's intelligence and security enterprise. Further, a Minister for Intelligence as an elected official would be able to engage with their parliamentary party room, the opposition, cross bench,

and the public to advocate reforms and changes in a way a public servant simply could not. This is a much-needed role when one considers the range of complex security laws and investments the Cabinet, the Parliament, and the public are being regularly asked to understand and support.

Alongside the urgent need to improve the executive leadership structures for Australia's intelligence and security system, is the equally important need to modernise the structures and resources of Parliament, especially the Parliamentary Joint Committee on Intelligence and Security (PJCIS).

Strengthening Parliament's Role

The PJCIS, as it is currently constituted, was formed in 2005 following the recommendations of the Flood Inquiry, which suggested all the agencies of the then Australian Intelligence Community should fall under the scrutiny of a single, dedicated joint committee of Parliament. However, the Committee's direct lineage goes back at least to the 1980's. Prior to the Flood Inquiry, the Parliamentary Joint Committee on ASIO, ASIS and DSD (PJCAAD) as it was, exercised a discreet remit over Australia's two primary foreign intelligence collection agencies and Australia's domestic security agency ASIO. This composition was a product of the Intelligence Services Act 2001 which added ASIS and DSD to the Committee's work as part of the rapid reform of following the strategic shock of 9/11.

From 1988 to 2001, the Parliamentary Joint Committee on ASIO had exercised much narrower oversight.

In other words the Committee was being pragmatically given ever-larger tasks for exercising scrutiny and oversight over Australia's shifting and expanding national security ecosystem. This expansion of the Committee's work was historically a prudent and logical adjustment to the expanding power of security institutions. Yet given existing resources we have arguably reached the limit to which this committee can reasonably consider such a varied agenda of work whilst still effectively holding agencies and their leadership to account.

The PJCIS has an impressive remit for inquiring into the activities and powers of national security agencies. In this regard it is similar to the Senate Select Committee on Intelligence and House Permanent Select Committee on Intelligence of the US Congress or the Intelligence and Security Committee at Westminster. However, the PJCIS differs from these bodies in some important ways that make it practically less powerful. For one, the PJCIS has less of a role than its American and UK counterparts to oversee or authorise the operational decisions of intelligence agencies. Its influence over agency budgets is minimal.

Further, the PJCIS comprises ordinary parliamentarians, many of whom sit on other committees and who must

use their small staffing contingent to manage multiple committee commitments as well as essential electorate matters. Upon joining the PJCIS, none of their staff are given high level security clearances to support them, meaning committee members cannot consult their own advisers in forming their assessments of Parliamentary business.

For example, members regularly receive classified briefings, but they cannot involve their own staff in considering such briefings.

Addressing this would be an easy way to bolster support for PJCIS members. Additionally, NIC agencies should be encouraged to second staff to the small PJCIS Secretariat within the Department of the House of Representatives that serves the Committee.

The limited support currently available to the PJCIS is an acute problem given the remit of the Committee's work.

The PJCIS is now dealing with arguably the most complex and arcane aspects of government business, especially for members who have had limited previous exposure to law enforcement, security or intelligence issues. For example, recently the Committee has been simultaneously considering inquiries into extremism and radicalisation, foreign intelligence collection, access to telecommunications data, the listing of terrorist organisations, the security of critical infrastructure, criminal use of the dark web, oversight reforms, and agencies' expenditure.

To ensure Parliamentary representatives receive more information about intelligence activities than what agencies tell them, the Government should implement the 2017 L'Estrange Review's recommendation that the PJCIS be given the remit to commission the Inspector-General of Intelligence and Security to undertake special reviews and investigations so that Parliament can gain access to operational insights on its own terms.

Such support would not be unprecedented, as the PJCIS has increasingly turned to the Independent National Security Legislation Monitor (INSLM) to support its reviews of particularly thorny legislative questions; for example in 2019 the Committee asked the INSLM to review Australia's regime for telecommunications companies assisting law enforcement and intelligence agencies. However, the INSLM is only a part-time appointee, usually a former judge, and not resourced to undertake more than a handful of reviews at once. Empowering the PJCIS to call on the IGIS to inquire into operational issues and the INSLM to review legislative reforms will ensure Parliament has the independent advice it requires to confidently scrutinise national security matters. Strengthening the PJCIS in this way could also reassure Opposition and crossbench members that they have satisfactory avenues to understand and contend government security policies.

A virtue of the PJCIS is that its decisions are made by consensus between all members, helping to shield its work from the partisan theatrics that can derail other Parliamentary business. However, the government of the day cannot be guaranteed of this good will convention if non-government members don't feel

as well appraised of the Committee's business. For this reason, access to independent advice from the IGIS and INSLM could reassure Opposition members on the PJCIS they are getting the information they need. This is no trivial concern. As ASIO has warned, Australia's politicians and institutions are increasingly being targeted by foreign actors hoping to discredit Australia's model of democratic governance and undermine Australia's solidarity on security issues by sewing discord and confusion.

This paper has outlined a range of practical recommendations for refining the capacities of Australia's political leadership to direct, oversee, and address contemporary security matters. It has been argued that Cabinet's ability to direct Australia's complex national security and intelligence apparatus can be strengthened through the appointment of a Minister for Intelligence. The paper has also laid out how Parliament's keystone security and intelligence committee, the PJCIS, can be made more effective at its work by being given new resources and powers. These reforms should be considered in earnest to ensure the institutions of Australian democracy are modernised for the security challenges of the twenty-first century.

Endnotes

1. Allan Gyngell and Michael Wesley, *Making Australian Foreign Policy* (Cambridge: Cambridge University Press, 2007), 146.
2. The Australian Secret Intelligence Service (ASIS), Australian Security Intelligence Organisation (ASIO), the Office of National Intelligence (ONI), the Australian Signals Directorate (ASD), Defence Intelligence Organisation (DIO) and the Australian Geospatial-Intelligence Organisation (AGO).
3. The Australian Criminal Intelligence Commission (ACIC), Australian Transaction Reports and Analysis Centre (AUSTRAC) and the Australian Federal Police (AFP).
4. Including: ASIO, ASIS, ONI, DIO, AGO, ASD, ACIC, AUSTRAC, AFP, the Australian Defence Force, Australian Border Force, Australian Government Security Vetting Agency, the Department of Defence, the Department of Home Affairs, the Department of Foreign Affairs and Trade, and the Department of Prime Minister & Cabinet.
5. Philip Flood, *Report of the Inquiry into Australian Intelligence Agencies* ([Canberra: Dept. of the Prime Minister and Cabinet, 2004).
6. The Australian Secret Intelligence Service and the Defence Signals Directorate (now the Australian Signals Directorate).
7. Commonwealth Parliament, Parliament House, 'History of the Intelligence and Security Committee', Australia, https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/History_of_the_Intelligence_and_Security_Committee.
8. '2017 Independent Intelligence Review', Commonwealth of Australia 2017.
9. James Renwick, Australia, and Independent National Security Legislation Monitor, *Trust but Verify: A Report Concerning the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 and Related Matters*, 2020.
10. 'Director-General's Annual Threat Assessment', 17 March 2021, <https://www.asio.gov.au/publications/speeches-and-statements/director-generals-annual-threat-assessment-2021.html>.

About the Author

Dr. William A. Stoltz is the Senior Adviser for Public Policy at the National Security College. He is responsible for mobilising the College's research and resident expertise to influence and inform current public policy debates. Dr. Stoltz's own research explores options for Australia to shape and influence international security, as well as Australia's policy responses to a breadth of domestic national security challenges. He joined the NSC after working across Australia's defence, intelligence, and law enforcement communities, including strategic intelligence and advisory roles within the Department of Defence, the Australian Federal Police, and the National Intelligence Community.

E national.security.college@anu.edu.au

W nsc.anu.edu.au

 @NSC_ANU

 National Security College