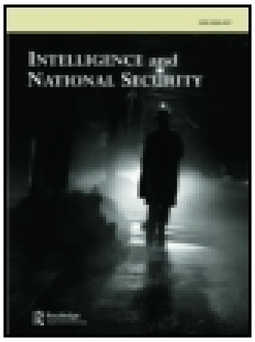

Intelligence and National Security

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/fint20

Transforming the Australian intelligence community: mapping change, impact and challenges

Patrick F. Walsh

To cite this article: Patrick F. Walsh (2020): Transforming the Australian intelligence community: mapping change, impact and challenges, Intelligence and National Security, DOI: 10.1080/02684527.2020.1836829

To link to this article: https://doi.org/10.1080/02684527.2020.1836829

Published online: 20 Oct 2020.

INTELLIGENCE AND NATIONAL SECURITY
https://doi.org/10.1080/02684527.2020.1836829

ARTICLE

Transforming the Australian intelligence community: mapping change, impact and challenges

Patrick F. Walsh

ABSTRACT

9/11 produced significant changes to the US intelligence community, while in contrast the attacks resulted in incremental changes in the Australian intelligence community (AIC). Fast forward to 2017 however, this article examines how the 2017 Independent Intelligence Review has created the momentum for significant change in the AIC; and what challenges may arise from reform initiatives flowing from the review. While assessing the full impact of the current reform agenda will take years, this article assesses key changes made so far (2017 to October 2020) and if they are resulting in a more effective, coordinated and integrated intelligence community.

Introduction

This article explores how the 2017 Independent Intelligence Review is currently setting the agenda for major reform of Australia's Intelligence Community (AIC). It investigates key Review recommendations and how these are being translated into a reform agenda currently underway in the AIC. In particular, the article asks two questions: what is the significance of the reform agenda now underway compared to other historical reform efforts; and what are the signs so far that this agenda is likely to yield a more effective, coordinated and integrated community? Before exploring both questions, it is necessary first to place current reform efforts into their historical context, particularly for non-Australian readers not familiar with key reform and developmental milestones of the AIC.

Historical context

The objective here is not to provide a detailed history of all changes in the AIC leading up to 2017. Readers wishing to drill down on specific events can do so by exploring relevant references included.[1] What is offered is a brief survey of key historical landmark events, issues and policies from 1945 up to 2017 that link past reform milestones with the contemporary reform agenda.

Cold War to 11 September 2001

Starting a brief historical overview of the AIC at 1945 may seem arbitrary since there were some semblances of at least parts of what was to become the community prior to the conclusion of World War 1; and in the decades between World War 1 and 2.[2] However, 1945 is a more appropriate time to start surveying the beginnings of a modern AIC as it aligns with developments in the intelligence communities of key 'Five Eyes' partners, who (particularly the U.S. and UK) were to have significant influence on its development.[3] Several historical accounts underscore the important implications that arose from the United States and its Anglosphere partners being victors in World War 2. Such

CONTACT Patrick F. Walsh pawalsh@csu.edu.au

close military cooperation became a bedrock upon which 'Five Eyes' countries were able from 1945 onwards to build deep trusting relations and common capabilities. Trust of course was forged (though not always maintained) at the political leadership level, but also at the intelligence officer to officer liaison levels. Arguably from an intelligence perspective, the most profound legacy of World War 2 was the creation of the vast global SIGINT alliance known as UKUSA – a treaty signed between Britain, US, Canada, Australia and NZ originally in 1948, which has deepened significantly since.[4]

While the UKUSA treaty was a significant stake in the ground for fostering trust and sharing of intelligence between partner countries, it also had the effect of pushing greater domestic capability building amongst treaty countries – particularly in Australia and New Zealand. For example, in the 1950s, both the US Truman and UK Atlee governments were concerned about KGB penetration in Australian politics, bureaucracy and society. There were leaks of highly sensitive material from the Department of External Affairs in Canberra to the KGB. London sent senior MI5 staff to Australia to pressure the Chifley government to deal with Soviet espionage in Canberra and create their own MI5 later known as the Australian Security Intelligence Organisation (ASIO) in 1949.[5] Some senior MI5 staff stayed on afterwards in the new ASIO. Shortly thereafter in 1952, the Liberal government of Robert Menzies without public knowledge approved the establishment of the Australian Secret Intelligence Service (ASIS) to gather information abroad about threats to Australian security.[6] Other key agencies of the AIC were established during the late 1940s and early 1950s in the Australian Defence Force, including the Defence Signals Bureau in 1947, which was later renamed the Defence Signals Directorate (DSD) in 1978 – and most recently the Australian Signals Directorate-ASD in 2013.[7]

Other military components of the AIC included the establishment in 2000 of the Defence Imagery and Geospatial Organization (DIGO), which was an amalgamation of three earlier agencies: the Australian Imagery Organisation (AIO), the Directorate of Strategic Military Geographic Information and the Defence Topographic Agency. Like ASD, DIGO was renamed the Australian Geo-Spatial Organization (AGO) in 2013. Finally, in the Defence portfolio, is the Defence Intelligence Organization (earlier referred to as the Joint Intelligence Organization). All three defence intelligence agencies (ASD, DIO and AGO) were derivative products of the Cold War.

By the early 1950s, most of the agencies that make up the current AIC had been established except the Office of National Assessments (ONA), which was set up by the Liberal-National Coalition government of Malcolm Fraser following a recommendation by Justice Hope's Royal Commission on the Intelligence Services that the AIC needed a centrally located and independent assessment function that was not the captive of one strong department such as the Defence Department.[8] Arguably, before the 2017 IIR, the 1977 Hope Royal Commission was the greatest catalyst for change within the AIC as it sought to address growing tensions between different agencies and deal with what Justice Hope referred to as fundamentally a 'fragmented, poorly coordinated and organised' (intelligence community) that 'lacked proper guidance, direction and control.'[9] To remedy this, the Fraser government established the Office of National Assessments (ONA) in 1977. The ONA was to provide all sources assessment advice and oversight of the AIC reporting directly to the Prime Minister.

Another significant outcome of the second Hope Royal Commission's report (1984) was the government's decision to create the office of the Inspector General of Intelligence and Security (IGIS) in 1985, which was designed to be a powerful and independent oversight body into the AIC.[10] The combination of the two major judicial reviews and the later enactment of the Intelligence Services Act 2001 all served to promote greater accountability and transparency over time in the functions and responsibilities of various AIC agencies. In addition to broadly prescribing the powers of ASIS, AGO and ASD, the Intelligence Services Act 2001 also established the Parliamentary Joint Committee on Intelligence and Security (PJCIS) to review the administration and expenditure of ASIO, ASIS, AGO, DIG, ASD and ONA, and make recommendations to the relevant ministry.[11] The

PJCIS however, unlike the US Senate Select Committee on Intelligence and its House (HPSCI) equivalent does not conduct any classified hearings into AIC operational matters.

In summary, the key milestones discussed above underscore a gradual evolution of the AIC from the early post-war years, throughout the Cold War and up to 9/11. Like other 'Five Eyes' partners, this evolution arose from the impact of several variables, including geo-political developments, innovation and technology that improved collection and other capabilities as well as internal political and bureaucratic policy development. As noted, the Hope Royal Commissions produced significant change in the coordination and accountability mechanisms in the AIC. Both commissions created the modern bedrock of the AIC upon which the community did not fundamentally shift from for the remainder of the Cold War and arguably into the post 9/11 period as well.

Post 9/11 to 2017

After 9/11 however, and shortly followed by other global and regional security events such as the Bali bombing of October 2002 and the London attack of July 2005, non-state actor threats were now vying for the attention of successive Labor and Liberal coalition governments in Australia. In particular, for the political leadership in Canberra, it was clear after 9/11 that terrorism was no longer a nuisance low impact crime, but rather a growing existential threat–one that remains a top national intelligence priority to this day. While the events of 9/11 were concerning to Australia's political leadership, of greater focus was the regional dimension of the terrorism threat. Concerns became especially escalated after the 12 October 2002 Bali Bombing, which killed 202 people–88 of them Australian citizens. The attack was authored by Indonesian terror group Jemaah Islamiyah (JI), but there was also growing concerns about other regional groups such as the Philippines Abu Sayyaf. The rise of JI and other regional terrorist groups in the initial few years after 9/11 demonstrated that the AIC and Australian police did not have a deep understanding of such regional threat actors, including their links to al-Qaeda.[12]

In the aftermath of the Bali attacks, the Howard Government made several political and policy decisions at the national, regional and international levels about how to manage the growing terrorism threat to Australian interests. Space limitations prevent a full discussion of all these.[13] However, in short order after the Bali bombings most member agencies of the AIC received a funding boost to increase counter-terrorism capabilities. Of particular, note the Australian Federal Police (AFP), which prior to 9/11 did not have a large counter-terrorism capacity saw the equivalent of a doubling of its budget to AUD 500 million after 9/11.[14] Also in 2004 at the national level, the Department of Foreign Affairs and Trade (DFAT) produced a white paper on terrorism, which was an early attempt to articulate a whole of government strategy to counter-terrorism.[15] At the regional level, MOUs were struck initially with Indonesia and Malaysia to counter-terrorism and to increase joint police and intelligence counter-terrorism efforts. At this time also Australia's participation in the invasion of Afghanistan in 2002 and Iraq in 2003 also highlighted the ongoing threat to Australian interests from terrorism and the need for further investment in the AIC's collection capabilities. Important as non-state actor threats (such as transnational and regional jihadist threats) had come in the first few years after 9/11 however, government efforts to increase IC's capabilities in response did not result in a wholesale rethink of the Community's structure.

Even in 2004, when the government commissioned the Flood Report to examine various aspects of the AIC including its performance in assessing Iraq's WMD capabilities prior to the coalition invasion in 2003; and its understanding of regional terrorism groups such as JI–there was no major community-wide restructure recommended by the reviewer Philip Flood. Flood choose to stick to reviewing the AIC's foreign intelligence capabilities and not how these interacted with domestic intelligence or the wider law enforcement community.[16] The latter and additional focus would have provided a more comprehensive review. In the main though, Flood concluded that the architecture designed by Justice Hope in the 1970s for the AIC remained valid, and there was no need for fundamental structural change.'[17] Importantly though, Flood did recommend further reviews of the AIC in a period every 5 to 7 years. Since 2004 governments of both political persuasions have commissioned two additional independent inquiries into the AIC. The next occurred under the Gillard Labor government in 2013 – and the third the subject of this article – the 2017 IIR – occurred in 2017 under the Turnbull Liberal-National Coalition government.

In 2007, after the conservative Howard Government was voted out of office, there was again momentary speculation that the incoming new Labor government of Prime Minister Kevin Rudd may embark on a radical structural overhaul of Australia's national security arrangements. Rudd intimated as much prior to forming government that a major redrafting of the national security architecture was possible – and rumours abounded that this might mean the creation of a U.S. style Department of Homeland Security or even the equivalent of an 'Australian ODNI.' Rudd tasked Ric Smith a former Ambassador to Beijing, who also had senior appointments in the Departments of Foreign Affairs and Trade and Defence to review current national security arrangements.[18]

In the end the Smith Review, discounted the need for a U.S. style DHS or the creation of an ODNI supra agency to provide stronger coordination across the AIC and law enforcement agencies. Instead, Prime Minister Rudd during his First National Security Statement delivered to parliament in December 2008, opted for stronger coordination of current arrangements through the Department of Prime Minister and Cabinet. This included the creation of a new office of the National Security Adviser within the prime minister's department, to provide strategic direction and support a 'whole-of-government national security policy.'[19] Other minor AIC structural change saw the establishment in 2011 of the Counter-Terrorism Control Centre (CTCC) housed in ASIO to overcome some siloing of information seen in National Threat Assessment Centre and promote more efficient identification of intelligence and investigative priorities.[20]

However, for the most part, as noted earlier, legislative activism, increased funding and the establishment of additional coordination arrangements were the three main responses by successive governments to any AIC reform from 9/11 up until the Turnbull Liberal-National Coalition government's commissioning of the 2017 IIR.

From the legislative perspective, there was a proliferation of counterterrorism and intelligence-related legislation from 2001 to the present. In the first decade alone after 9/11, 54 pieces of anti-terrorism legislation were passed by the federal parliament and many of these increased the powers of AIC agencies such as ASIO and AFP to hold and question suspects for longer periods before being charged and to control the movements of others.[21] Much of this legislation as noted earlier was passed during the government of Prime Minister John Howard (1996–2007). The Labor government years of Prime Ministers Rudd, then Gillard and Rudd again (2008–2013) were less active in the legislative area, but the cumulative effect of all legislation enacted by successive governments has been a larger suite of powers for the AIC compared to most other 'Five Eyes' partners. Legislation has provided the AIC with extensive powers to operate in more flexible and proactive ways to prevent and disrupt particularly terrorists' threats than arguably exist in other 'Five Eyes' partners.[22]

There is insufficient space to get into the specifics of legislation enacted from 2001 to the present. But as a general rule AIC agencies were given additional collection and operational powers as governments perceived threats both on and offshore evolving. For example, as concern moved away from al-Qaeda to the expansion of the Islamic State (IS) in Iraq and Syria in 2014 a further suite of legislation was enacted by the incoming conservative Abbott and Turnbull governments. For example, the Counter-Terrorism Legislation Amendment (Foreign Fighters) Act (2014) was designed to prevent young Australians suspected of being radicalised jihadists travelling to proscribed areas of concern in the Middle East including the IS Caliphate in Syria to fight for IS. Other notable legislation passed included *the National Security Legislation Amendment Act (2014*), and *the Telecommunications (Interception and Access) Amendment (Data Retention) Act (2014)*. Both were significant enhancements of Australia's national security and intelligence collection capabilities–arguably not seen since the Howard Government in 2007'.[23] Importantly though the proliferation of legislation did not prompt governments into any systemic and structural reconfiguration of the AIC rather it expanded the powers of existing agencies.

Though at this time, an accumulation of over 15 years of either amended or new counter-terrorism and intelligence legislation started to raise concerns by the federal opposition and the public about the impact of enhanced surveillance and more prescribed measures in the Foreign Fighters Act that were also seen to restrict public speech that might be interpreted as supporting terrorism.[24] Concerns were compounded in the community following the Edward Snowden revelations about the scale and various methods used by the NSA and its other 'Five Eyes' equivalents such as Australia's ASD.[25] WikiLeaks had already precipitated a greater political and community debate in Australia about the role of intelligence, surveillance and privacy.[26] However, the June 2013 Snowden leaks had a catalytic effect on this debate, particularly when it was revealed the AIC was spying on senior members of the Indonesian government including on behalf of the NSA during US-Indonesian trade talks.[27]

From 2013 onwards, increasing debates in the Australian media and community emerged about the application of counter-terrorism laws by various AIC agencies and whether they were appropriate, proportionate and legal. Though the seeds of growing community concerns were already in place by the mid-2000s when the AFP detained and arrested Dr Mohamed Haneef for his alleged role in failed attacks on a London nightclub and Glasgow airport in July 2007. A subsequent judicial inquiry (the Clarke Inquiry) into the matter found the evidence against Haneef 'completely deficient' and that ASIO had informed the AFP that there was no evidence to suggest Haneef was 'guilty of anything'.[28] Ultimately, Clarke concluded that AFP Commander, Ramzi Jabbour, manager of Counter-Terrorism Domestic, had 'lost objectivity' and was unable to see that the evidence he regarded 'as highly incriminating amounted to very little'.[29] Clarke recommended parliament implement oversight of the AFP and reform the counter-terror legislation.[30] Similarly, an internal review commissioned around the same time as the Clarke Inquiry (the Street Review) of the AFP counter-terror practice identified a failure of 'interoperability between the AFP and its national security partners'[31] But yet both the Flood inquiry discussed earlier nor the government responding to the Clarke Inquiry saw any urgency to look at how AIC agencies were using an ever increasingly complex suite of counter-terrorism legislation and whether any structural change to the AIC would help remedy operational deficiencies in how legislation was being applied.

In addition to the enactment of a large volume of counter-terrorism and intelligence-related legislation, a second strategy used by successive governments from mid-2000 to the present to improve AIC capability has been increasing agency headcount and operational capability.[32] For example as the 2015 Review of Australia's Counter-Terrorism Machinery noted, between 2001 and 2014, the budget for ASIO increased more than fivefold; that of the ONA almost quadrupled; for ASIS it more than tripled and for the AFP it more than doubled.[33] Meanwhile, recruitment to the AIC also rose dramatically. ASIO's staff increased from 600 officers in 2002 to 1980 by the 2017–18 financial year.[34] AIC funding fell a little after the Labor government's review of counter-terrorism in 2008 – though mounting concern about the internal and external threat posed by the rise of Islamic State saw Tony Abbott's Liberal-National Party coalition government increase the AIC budget by a further AUD 634 USD million in 2014.[35] This investment represents a significant long-term commitment to placing intelligence security at the forefront of the government response to the new risk environment.

This increased investment in AIC capability by the incoming Abbott Government was based on an assessment by cabinet that the threat from global Islamist terrorism was growing and becoming even more diverse and complex.[36] While Al-Qaeda's central network was disrupted, its many franchises in the Arabian Peninsula, the Maghreb, and in Iraq and Syria were still active. The political instability in Iraq following the US drawdown of troop in 2009 and the civil war in Syria also led to the evolution of ISIS from Abu Musab al Zarqawi's al-Qaeda in Iraq, whilst the al-Nusra Front took shape in Syria after 2012. As mentioned earlier, the desire of radicalised western youth to take part in the IS struggle against Iraqi, Syrian regimes and western coalition military forces proved great. IS also became more sophisticated than Al-Qaeda in its use of digital communications that facilitated global recruitment, operational planning and propaganda. In particular, IS became very skilful in recruiting or inspiring lone actors to carry out attacks in European cities, the US, Canada and Australia. As the IS Caliphate consolidated its physical and virtual power, the AIC and its 'Five Eyes' partners began to increasingly struggle in collecting and disrupting against a new kind of counter-terrorism threat – particularly marked by random lone actor attacks with little or no warning.[37] While the AIC and other 'Five Eyes' ICs have invested heavily in monitoring IS and other jihadist social media communications, the interception, decryption and analysis of social media remains an ongoing capability challenge.[38]

The emergence of Islamic State in 2014 and 'lone actor attacks' in Melbourne and Sydney discussed earlier coincided with Tony Abbott's new Liberal-National Coalition government (2013–-2015) and resulted as described above in a further review of security, as well as the promulgation of new laws to address the phenomenon of foreign fighter recruitment and online 'radicalization'. Yet none of these measures including those implemented during the Labor Rudd/Gillard/Rudd Governments resulted in significant structural reform of the AIC. On the whole, policy and legislative reforms tended to be more adhoc in responding to external geopolitical events. Enhanced coordination efforts, funding and legislation seemed to be generally the prescription offered rather than any contemplation of a wholesale rethink of the Australian intelligence enterprise.

This approach begun to change, however, when in November 2016, Prime Minister Malcom Turnbull announced the commissioning of a third independent intelligence review – the other two occurring in 2004 (Flood Report) and 2011 (Cornall and Black Report) respectively.[39] Two respected senior bureaucrats, Michael L' Estrange and Steven Merchant were appointed reviewers. The Prime Minister's media statement briefly outlined the broad objectives of the review though little detail was given publicly about any specific concerns the government had on the AIC's performance. Rather the language of the media statement implied the government was looking for a 'health check' rather than a root and branch review. Unlike the Flood Report, there was no pressing intelligence failure needing investigation, but unlike Flood – the 2017 IIR proved to be more comprehensive in reaching out to AIC agencies, political leaders, other AIC customers and the community for consultation.[40] The reviewers identified several coordination, funding, IT, legislative, and accountability issues that could be strengthened in the AIC. Limited space does not permit a full analysis of all 23 recommendations listed in the 2017 IIR report. Instead, the remaining part of this article will focus on recommendations 1, 3, 14,15 and 21 to 23. Combined they provide a good indicator of both the significance of reform measures articulated in the report and allow some preliminary assessments on whether they will likely result in greater coordination, integration and effectiveness across the AIC enterprise.

The 2017 independent intelligence review and key recommendations

The most important recommendation (number 1) was that an Office of National Intelligence (ONI) be established as a statutory body within the Prime Minister's portfolio. In the report's executive summary, the reviewers made it clear that 'excellence' overall defined the AIC's activities, yet an even higher level of performance was possible through further strengthening integration across agencies. What was missing they concluded was a stronger coordination of the intelligence enterprise similar to efforts made they argued by intelligence communities in the U.S and UK post 9/11.[41] Their remedy for enhanced integration and performance was recommending the creation of ONI– headed by a Director-General, who would become the Prime Minister's principal adviser on matters relating to the national intelligence community. The Director-General would not be given the powers to direct specific functions and activities of agencies but would be responsible for the co-ordination of the AIC to ensure there existed an appropriately integrated approach across the suite of agency capabilities.

ONI would also be given the responsibility for enterprise-level management of the AIC which includes: 'leading the development and implementation of national intelligence priorities, undertaking systematic and rigorous evaluation of the performance of the agencies, implementing strategic workforce planning and facilitating joint capability planning; including for the development of an environment for enhanced data sharing and collaborative analysis.'[42] ONI would subsume the Office of National Assessments–the all source assessment agency established in 1977 and undertake its intelligence assessment function in an expanded way that included greater contestability and more extensive engagement with external expertise.[43]

The second most important recommendation (number 3) identified by the Reviewers is the establishment of the position Deputy Director General (ONI): Intelligence Enterprise Management, who would be responsible for leading the many enterprise-level management responsibilities mentioned in the last paragraph. This executive role would also be expected to facilitate closer coordination, evaluation and integration of key intelligence missions such as cyber security and counter-terrorism intelligence. Although the former ONA played a central role in the coordination of various AIC intelligence activities, adding formally integration and evaluation functions signalled an expectation by government that ONI was to have a more prescribed role in how the AIC as a whole was working and reporting this back to government regularly.

Thirdly, there were four recommendations (15,21–23) relating to various oversight and accountability matters. The first (recommendation 15) suggested to government a comprehensive review of legislation governing the AIC. Recommendation 21 argued for an expansion of the oversight roles of both the Parliamentary Joint Committee on Intelligence and Security (PJCIS); and the Inspector-General of Intelligence and Security (IGIS) to apply to all 10 agencies within the AIC. This long-overdue expansion of IGIS's remit means it will now have (once the IGIS Act 1986 is amended) oversight of the intelligence functions of four additional agencies: the Australian Federal Police, the Department of Immigration and Border Protection, the Australian Criminal Intelligence Commission and the Australian Transaction Reports and Analysis Centre (AUSTRAC). The other two (recommendation 22 and 23) were also overdue, but once implemented will result hopefully in a material improvement in AIC oversight and accountability.

Recommendation 22 advised the government to increase full-time staff at the IGIS to at least 50 – allowing more frequent and deeper inspections of AIC operations.[44] Similarly, an expanded oversight role for the Parliamentary Joint Committee (PJCIS) was suggested by the Reviewers, where the Committee will now be able to request the IGIS to conduct an inquiry into the legality and propriety of operational activities and provisions within the AIC as well as allowing the PJCIS to initiate its inquiries into-the administration and expenditure of the now 10 intelligence agencies. Both measures are not insignificant, but they do not allow the PJCIS to conduct classified hearings into operational matters within the AIC.

The final noteworthy recommendation (no 14) was a suggestion by the Reviewers that ONI needed a more structured and strategic approach to identifying responses to changes in science and technology that impact the AIC. Two remedies were identified. One related to the establishment of a National Intelligence Community Science and Technology Advisory Board and the other was the creation of a National Community Innovation Fund to support research that addressed capability needs and solutions.[45] Related to building capacity was a further recommendation (number 7) that a joint capability fund be established to support technological innovation and the development of shared capabilities. The idea being that the fund could help government plan more strategically regarding future capability gaps. The next section summarises how the above seven recommendations have been operationalised and their impact on the AIC so far.

Operationalising key review recommendations

Recommendation 1 creation of ONI

The government accepted all the recommendations of the 2017 IIR report upon its release in June 2017. The most important of these as noted earlier was the establishment of ONI from its predecessor agency the ONA. This required new legislation: The *Office of National Intelligence Act*

2018 passed in December 2018. ONI's predecessor ONA had always been a small (approximately under 100 pre-2017) largely assessment-focused agency. With ONI's enhanced mandate, particularly in intelligence enterprise management – ONI's headcount is expected to roughly triple to about 300 staff over the next few years (2020–2023).[46] ONI's headcount is also being supplemented by transfers from other AIC agencies and staff, who previously worked in the national security intelligence section of the Department of Prime Minister and Cabinet. In addition to hiring staff to fulfil the new enterprise management function ONI has moved into expanded accommodation.

Recommendation 3 ONI's new enterprise-level management role

Since its establishment in December 2018, ONI has also taken concrete steps to implement various initiatives and processes relevant to carrying out its new and legislatively mandated enterprise-level management role of the AIC. For example, it has established mission intelligence groups (MIGs) each focusing on a particular Australian intelligence mission priority set by government. The MIGs are led by a mission manager and a number of staff, who can help identify collection, assessment and capability gaps across the community–thereby providing a more coordinated and deconflicted approach. As noted earlier, the now expanded AIC consists of 10 agencies rather than the six prior to the review. The new coordination arrangements through the MIGs should begin to streamline areas where there currently is insufficient coordination particularly around collection and assessment capabilities–human or technical.

Each MIG is led by a middle-ranking intelligence officer. However, care is needed to ensure there is a good mixture of different AIC agencies personnel leading various MIGs with the appropriate expertise rather ONI attempting to lead them all. Although the new MIG structure will likely improve coordination and integration on mission priority areas, mission managers, however, do not have expressed authority to mandate agencies to collaborate on mission collection priorities. It is likely in significant mission priority areas such as China or cyber, MIGs will promote enhanced coordination and integration of collection and assessment capabilities. Though perhaps for lower mission priority areas mission managers in ONI will need to demonstrate adeptness in 'herding' various already resource strained AIC agencies to work together.

Though progress has been made in establishing MIGs, it is less clear how ONI will progress its broader suite of enterprise-level management coordination and integration roles across the AIC. For example, in more conventional threat spaces such as counter-terrorism, ASIO has led in the coordination, integration and priority setting of the AIC response effectively. So, it is unclear how ONI will value add to existing arrangements in ways that facilitate closer coordination and integration in a number of cross AIC efforts.

Nonetheless, it is clear that de-confliction in coordination and integration of intelligence activities may need to occur between AIC agencies in the future on some mission areas. The greater potential concern in the short to medium term is how ONI goes about its enterprise management role when another recently established super-ministry–the Department of Home Affairs (DHA) also has within its mandate an intelligence coordination role. The DHA was created by the Liberal-National Coalition Turnbull Government on 20 December 2017. It brings together the Australian Border Force (ABF), the Australian Federal Police (AFP), the Australian Criminal Intelligence Commission (ACIC (including the Australian Institute of Criminology)), the Australian Security Intelligence Organisation (ASIO), and the Australian Transaction Reports and Analysis Centre (AUSTRAC). The DHA includes the entirety of the former Department of Immigration and Border Protection and functions that came from other Departments relating to multicultural affairs, emergency management, transport security, transnational serious and organised crime, criminal justice policy, national security and counter-terrorism coordination, cyber policy, and countering foreign interference.

Each of the six DHA participating agencies maintain their statutory independence rather than being formally dissolved. The official government rationale for creating a super department was posited the following way in its first Annual Report:

> 'the portfolio brings together the strengths of each individual agency in a synthesis that is stronger than any constituent part could be. 'The Portfolio is structured to benefit from the collaboration and alignment of sustained joint-agency effort.' 'Through even closer cooperation and sustained joint activity between our national security and law enforcement agencies, including federal, state and territory government agencies, the Portfolio will continue to coordinate and drive national efforts against terrorists, criminals and others who wish to harm the Australian community.'[47]

It is clear that both the creation of ONI and the Home Affairs portfolio combined represent significant reforms to not just national security, but also to the broader federal law enforcement architecture. But the establishment of the DHA has been more controversial than the creation of ONI. The federal opposition party (the Labor Party), media reporting and some quietly in the intelligence community have criticised the need for the creation of a super ministry, which essentially puts key federal law enforcement agencies (AFP and the ACIC) together with Australia's domestic security intelligence agency ASIO. Criticisms have included that combining all these agencies under the one minister instead of the previous three or four invest a single minister with enormous power. There was also a political dimension to its establishment with the former and deposed Prime Minister Malcolm Turnbull creating it to help assuage the political ambitions of its newly appointed minister Peter Dutton. In summary, an argument can be made that the creation of the DHA was an attempt by government to fix 'coordination issues' between federal law enforcement and national security intelligence agencies that didn't exist. Indeed, less than 2 years before DHA was established, even the government's 2015 commissioned Review of Counter-Terrorism Machinery argued against its creation–saying 'it was not an optimal response to the terrorism threat and might end up privileging domestic over international elements of the problem.'[48]

Since its establishment in 2017, however the DHA has set up several new coordination functions for Transnational, Serious and Organised Crime and Counter Foreign Interference. DHA has also moved the Commonwealth Counter-Terrorism Coordinator and the National Cyber Security Advisor into the department. But it is less clear from its inception the kind of leadership role the department wishes to play in the intelligence coordination and broader enterprise management space. DHA when first established stood up an intelligence and capability group, which suggested it had ambitions to lead coordination efforts between federal law enforcement agencies and wider AIC. Though in the last two years (2018–2020), DHA's executive have struggled to demonstrate how a new super ministry can value add to existing AIC and law enforcement intelligence coordination beyond what its individual agencies such as ASIO and the AFP already do. Somewhat tellingly that the DHA's intelligence leadership aspirations are being adjusted, its most senior intelligence official–the deputy secretary for intelligence capability group left the department in 2019. The intelligence function now seems to have been given less prominence and has been subsumed into an entity called 'Technology and Major Capability Group'.[49] At the time of writing this downgrading of the DHA, intelligence coordination function suggests the super-ministry is focusing more on playing a policy rather than intelligence coordination and integration role in the AIC.

There is currently no evidence that any intelligence coordination, integration and capability focus DHA has at this point is conflicting with the formal legislated enterprise management role ONI was given in the ONI Act 2018. Nonetheless, the work DHA does on intelligence coordination through its taskforces and intelligence capability development (e.g. training programs, science and technology initiatives) could in the future cut across similar enterprise management initiatives driven by ONI. This could result in similar or different intelligence coordination, integration and capability initiatives developed by ONI and DHA that waste or duplicate resources–resulting in less integration and coordination across the AIC.

The Director General ONI and the Secretary of DHA will need to identify mutually agreed governance arrangements to ensure ONI continues to play the central enterprise management role of the AIC, yet allows the DHA and its agencies to identify integration, coordination and capability measures that best work for its agencies. ONI/DHA governance arrangements for instance need to address questions such as what coordination role should ONI have if any in areas such as counterterrorism, cyber, foreign interference and AIC training and education compared to DHA or the role of individual agencies?

Recommendation 14 a new enterprise-wide science and technology role for ONI

As noted above, recommendation 14 suggested that as part of its new enterprise management role, ONI needed a more structured and strategic approach to identifying the impact of changes in science and technology on the AIC. Since 2018 ONI has made some progress in this area by establishing the National Intelligence Science Advisory Board (NISAB). The NISAB currently includes representatives from all NIC agencies and invited senior researchers from a range of Australian research institutes and universities. At the time of writing its focus seems mainly on STEM disciplines; and the Board's terms of reference are yet to be finalised.

Another related area, however, where more progress has been made by ONI is the establishment of a joint capability fund for the AIC (2017 IIR recommendation 7). All AIC member agencies pay into the joint capability fund and can apply for larger funds to support gaps in technological innovation, training and other workforce development. AIC agencies on applying for funding must demonstrate how their project will help not only their agency but improve overall AIC capability. There have been three joint capability funding rounds since ONI's establishment though details of what gets funded is classified at SECRET or above.

Recommendations 15, 21-23 expansion of intelligence legislative and oversight mechanisms

The final four recommendations (15, 21, 22 and 23) as noted above relate to reforms on the AIC's legislative and oversight mechanisms. Recommendation 15 called for a comprehensive review of Acts governing the AIC. This review commenced in May 2018 following the government's announcement that former Secretary of DFAT, Defence and Director Security (ASIO) Dennis Richardson AO will conduct a comprehensive review of the legal framework governing the national intelligence community.[50] Mr Richardson submitted a SECRET review report to government in December 2019 and AIC agencies are now considering its recommendations. At this stage, it is not clear when the AIC will provide government with its collective response to the review. It may take until the end of 2020 given the current operational tempo of AIC agencies and the government's overwhelming focus on COVID-19. As discussed earlier, since 9/11 successive Australian governments have introduced a significant tranche of legislation in areas such as counterterrorism, illegal immigration, organised crime and foreign interference that impact on AIC operations. A streamlining of national security intelligence legislation is warranted though at this time it is uncertain how the government will approach this and what impact any legislative reform will have on the AIC, including the implementation of other post-2017 Review reforms. Further clarity on how the government will simplify a crowded suite of intelligence legislation will emerge once it releases a public version of the Richardson Review.

Recommendations 21 to 23 focused on expanding the oversight role of the Parliamentary Joint Committee on Intelligence and Security (PJCIS) and the Inspector-General of Intelligence and Security (IGIS). Recommendation 21 dealt with the legislative changes required to expand IGIS and PJCIS oversight over the expanded 10 agencies within the National Intelligence Community. The key acts to be amended for the PJCIS is the Intelligence Services Act 2001 and for the IGIS Act 1986. At the time of writing, neither has been amended. The amendments are straightforward and nearly 3 years on from the 2017 Review should have been completed. It is difficult to speculate why there has been a delay. It is possible there is a backlog of legislative amendments given the government's current preoccupation with COVID-19. Parliamentary committee work and indeed parliament itself has been operating in a piecemeal fashion for most of the first half of 2020. But it is also possible that the government will wait until the AIC responds to recommendations from the Richardson Review and make amendments to all relevant intelligence legislation at this point.

Recommendations 22 and 23 are also consequential and once implemented should result in material improvement in AIC oversight and accountability. Recommendation 22 suggested to government that the principal independent intelligence oversight institution–the Office of the Inspector-General of Intelligence and Security (IGIS) be expanded in headcount in order to better manage an expanded oversight role of the now 10 AIC agencies. The Reviewers recommended to government that IGIS headcount be increased to 50 staff and the government has now provided funding for this increase.

Since early 2019, IGIS has been in the process of recruiting additional staff of 55 to take on the increased oversight role of 10 agencies. This will represent a tripling in numbers compared to pre-2017 IIR levels. Although IGIS Act 1986 has not yet been amended to allow for formal oversight investigations into all 10 agencies, the IGIS in the meantime has seconded staff to the new AIC agencies (e.g. AUSTRAC, the ACIC, AFP and DHA) it now has oversight for in order to build relationships with them. The IGIS annual reporting shows that while waiting for amendments to relevant operating legislation, the office has engaged in a number of organisational activities to better prepare for both an expanded and more complex workload. Importantly IGIS has begun a comprehensive review of internal governance arrangements, which amongst other things will look at the types of staff currently employed.[51] At the time of writing despite post Review progress in IGIS reforms however, the office cannot begin formal oversight reviews of all 10 agencies until it has been given the authority via the legislative amendments discussed earlier.

Finally, recommendation 23 suggested to government the expansion of the oversight role for the Parliamentary Joint Committee (PJCIS). The PJCIS will now be able to request the IGIS to conduct an inquiry into the legality and propriety of AIC operational activities and provisions and for the Committee to initiate its inquiries into the administration and expenditure of the now 10 intelligence agencies is a significant change. Again, the government accepted this broader mandate for the PJCIS. However, the government also agreed with the Reviewers that the IGIS should remain the key oversight body to conduct classified oversight of AIC operational activity rather than the PJCIS. In a submission to the 2017 IIR, the author argued that the PJCIS should be given this expanded role as an additional check and balance on the parliamentary executive and IGIS oversight activities.[52] However, the Reviewers did not recommend this change to government which would have put its mandate more in line with the legislative oversight bodies of other 'Five Eyes' countries such as the U.S Senate Select Committee on Intelligence and the House Permanent Committee on Intelligence– or Canada's National Security and Intelligence Committee of Parliamentarians (NSICOP).

In the end after some deliberation, the reviewers argued that giving the PJCIS this additional oversight power over sensitive operational matters would duplicate existing oversight provided by responsible ministers, the IGIS and the Independent National Security Legislation Monitor (INSLM).[53] The INSLM reviews independently the operation, effectiveness and implications of national security and counter-terrorism laws. The Reviewers argued that ministers were best to judge how effective agency operations are and be accountable for them to parliament. They added that the PJCIS can still look at matters once referred to them.[54] As a compromise on this potential increase in the parliamentary committees' oversight powers, the reviewers recommended instead that the Director-General, ONI and the IGIS should brief the PJCIS regularly. In addition, that the PJCIS should be given authority 'to request the IGIS to conduct an inquiry into the 'legality and propriety of particular operational activities of the NIC agencies.'[55]

Outlook

In this final section, the article returns to the two central questions posed earlier: are the post-2017 IIR reforms significant and are they improving coordination, integration and the effectiveness of the AIC? The first question is easier to address. It is clear that the 23 recommendations in the 2017 IIR and the associated reforms to date represent significant reform to the AIC likely not seen since Hope Royal Commission reforms of the 1970s and 1980s. Just implementing recommendation 1 alone is a significant reform as it resulted in the creation of the ONI and provided the AIC with a central agency with a legislatively prescribed role to monitor and promote enterprise management coordination, integration and capability development.

The main theme in the 2017 IIR Report was the need for a single point of coordination for the AIC and this has now been achieved. The Reviewers noting other 'Five Eyes' partners such as the UK and USA had taken steps to strengthen the coordination and integration of their intelligence communities saw the establishment of the ONI as the primary vehicle for building strong, 'strategic-level management of intelligence as a national enterprise built on the specific attributes of individual agencies.'[56]

But the 'significant reform measures' underway post the 2017 IIR at this point have not yet consistently translated into a more coordinated, integrated and effective AIC. The discussion above on how various recommendations have been operationalised suggest progress in the coordination and integration of some enterprise-wide functions and only modest improvement in others. For example, ONI's new intelligence enterprise management portfolio has made progress on formal intelligence coordination and priority setting processes through the MIGs.

However, in other ways ONI has failed to take a leadership role in coordinating and integrating AIC intelligence efforts at the strategic level. For example, in terms of providing intelligence support to relevant decision-makers during the COVID-19 pandemic ONI has not used this opportunity to credentialise its new enterprise management leadership role across the AIC. Instead other operational agencies in the AIC such as the ACIC, ASD and the Australian Defence Force have been more centrally involved in providing intelligence support to health authorities and the government. Arguably, ONI's limited role in responding to COVID-19 can be viewed as its first significant failure in its newly mandated enterprise management function. Hopefully though, going forward and after the acute phase of the pandemic ends it can begin to demonstrate a leadership role in the coordination and integration of health security intelligence for the AIC by creating, for example, a health security intelligence MIG.[57] There will be other emerging threats and risks this decade and if ONI cannot get ahead of these threat trajectories to lead the AIC in coordinating and integrating intelligence collection, analysis and capability development – it will fail the aspirations of the 2017 IIR reviewers; and more importantly its legislative-mandated role of enterprise management.

Additionally several parts of the ONI Act 2018 (e.g. Division 2 Section 7(10(b); Clause 9(1)(b); Clause 9(1)(d)) give ONI authority to evaluate various AIC functions, particularly as they relate to whether AIC resources are being allocated appropriately; and assessing 'intelligence failure' within the AIC. At the time of writing however, it is not apparent how much progress ONI has made in developing evaluation metrics for a broad range of coordination, integration and capability development processes and activities across the AIC. Processes for evaluating the annual performance of some enterprise activities such as collection and assessment against mission priorities may be easier and quicker to implement than others such as developing metrics that all 10 agencies will agree on in areas such as workforce development or common IT systems. ONI's new enterprise management function has only been in existence for only 2 years. Nonetheless in the next two years, it will need to develop a range of evaluation metrics in collaboration with all 10 agencies that provide government with better audits of performance – yet are implemented with agencies buy in rather than being imposed on them. As noted earlier, an additional potential barrier to effective integration, coordination and also evaluation may be if the DHA sees a performance evaluation role for itself over and above what ONI is mandated to do.

Other areas where post-2017 IIR reforms have been made related to the establishment of a joint capability fund and a National Intelligence Science Advisory Board (NISAB). The effectiveness of the former seems more promising at present than the latter. The NISAB could potentially play a critical role in advising the AIC on capability development and identifying world-class researchers to work on filling capability gaps and advising on emerging threats and risks. However as noted, its current focus on STEM research while understandable is far too narrow given understanding threats/risks and building capabilities to respond require multi-disciplinary responses–including those from the social behavioural sciences.[58] In addition to getting the NISAB's terms of reference right, the Board needs to develop as a high-level strategic decision-making body that can identify short, medium and longer term research projects completed within the AIC and/or by external researchers. If it can become a serious strategic decision-making body rather than just another 'talk-fest' then it will contribute significantly to lifting the science and technology short-comings in the AIC identified by the 2017 IIR. Time will tell how useful the NISAB will be, but an effective and comprehensive approach to science, technology and capability development will also require ONI develop a broader academic outreach program similar to the one the Canadian Security Intelligence Service established over a decade ago. While individual agencies have a history of reaching out to external academics and researchers; the culture of secrecy in the AIC is still very strong overall. The desire and rhetoric by agencies to reach out to 'outsiders' to gain knowledge is there, but many agencies still fall back to playing it safe by seeking answers to problems internally or using only a few 'trusted' external partners. This has the effect of denying the AIC access to a broader and diverse range of knowledge and subject matter experts that can contest agency and enterprise biases. At the time of writing, it does not appear that ONI has moved towards developing an AIC wide academic outreach program. Such programs do take time to develop. However, ONI could start moving in the direction of an eventually fully developed academic outreach program by commissioning useful less costly initiatives such as inviting subject matter experts to webinar series to discuss a capability or emerging threat issue. In addition to being another way for the AIC to garner critical external knowledge on threats, academic outreach programs will also be important to supporting the enterprise management role ONI is mandated to do. In particular, a viable program could help ONI identify ways to adopt and coordinate enterprise-wide management strategies on training and workforce issues in collaboration with external training and higher education providers.

Finally, whether all 23 recommendations and the key ones discussed here are implemented in ways that result in a more effective, coordinated and integrated AIC does not just depend on progress ONI can make in the next 2 years (2020–2022), but also in reforms underway in legislation and oversight mechanisms. As noted, a major review of counterterrorism and intelligence-related legislation (the Richardson Review) has been completed and is now being considered by the AIC. A public version of the review is yet to be made available, which would provide insights into areas where legislative reform may occur. However, it is likely the principal intelligence legislation–the Intelligence Services Act 2001 which outlines the roles, functions, and powers of most AIC agencies will be modernised to provide a clearer set of provisions and usage of intelligence powers across the 10 agencies. There may even be a rationalising of several pieces of surveillance and telephone interception legislation and warrant application processes. However, it may take another 2 years (i.e. 2022) before accurate assessments can be made on how legislative reform might impact on the way the AIC operates. Several other oversight stakeholders, in addition to the government such as the INSLM, PJCIS and IGIS, and the public will all want to input into this wholesale legislative reform process–likely resulting in further delays in enactment of new legislation. In summary, the direction of the legislative reform process and how it will impact on ONI's role and the broader AIC is a key unknown variable at this stage.

Finally, how recommendations 21 to 23 are fully operationalised will also have longer term impacts on shaping the effectiveness, integration and coordination of the AIC as an enterprise. The 2017 IIR Reviewers have placed the predominant oversight of the expanded AIC on the shoulders of the IGIS rather providing any significant increased powers to the PJCIS. The IGIS overall has performed its oversight role well historically of the six original AIC agencies, but now there are new layers of complexities with four additional agencies which only have a partial intelligence function. With the government increasing the headcount at the IGIS, the oversight role is expected to expand significantly in the next few years. However, in order to provide a comprehensive oversight of the AIC, the IGIS will need to rethink its historical mission of mainly focusing on compliance to legislation to a much broader oversight mandate of ONI's enterprise management role. This means the IGIS will need to develop deeper and broader expertise beyond legislation to other areas of AIC performance such as use of technology, ethics, intelligence sharing, and NIC performance. In other words, effective oversight will rely on not just hiring more legal or policy people, but subject matter experts who can provide oversight on a broader range of intelligence and technical matters than in the past. In order to carry out successfully its expanded oversight role, the IGIS will need to build internal expertise that can independently report to government that ONI is providing reliable enterprise evaluations of AIC performance.

In summary, the 2017 IIR recommendations are now translating into significant enterprise reform efforts in the AIC not seen since the Hope Royal Commission days. However, 2 years since the establishment of ONI progress on implementation of many key recommendations remains slow. In particular, the 2017 IIR reviewers argued in their report that the AIC needed an uplift in coordination, integration as well as the ability to evaluate performance from an enterprise-wide perspective. In order to meet this expectation and that of government, ONI will need to make sustained progress particularly in several key recommendations discussed earlier. It will be critical for ONI to construct formal and informal governance arrangements with AIC agencies, including the DHA. It must also show a more agile capability in responding at the strategic level to emerging threats and lead the narrative on how the AIC should respond to them. Additionally, significant work is required in advancing other enterprise management initiatives in capability development, training, workforce planning, science, technology, research and academic outreach. The next 2 years should be sufficient time to demonstrate whether ONI can demonstrate a solid and 'value-added' enterprise leadership role over other AIC agencies in ways that results in a more integrated, coordinated and effective AIC.

Disclosure statement

No potential conflict of interest was reported by the author.

Notes on contributor

***Patrick F. Walsh*, Ph.D.**, is a former intelligence analyst who has worked in Australian national security and law enforcement agencies. He is an associate professor, intelligence and security studies at the Australian Graduate School of Policing and Security, Charles Sturt University, Australia. He has consults to government and his research focuses on a range of intelligence capability issues including governance, leadership, intelligence and ethics, biosecurity, health security and cyber. He is the author of *Intelligence and Intelligence Analysis*, Routledge, UK 2011; *Intelligence, Biosecurity and Bioterrorism*, Palgrave Macmillan, UK, 2018; and the forthcoming, *Intelligence Leadership and Governance. Building Effective Intelligence Communities in the 21st Century*, Routledge (due November 2020).

ORCID

Patrick F. Walsh http://orcid.org/0000-0002-1369-5468

Notes

1. On recent AIC reform studies see for example: Jones, "Intelligence and the Management of National Security: The Post 9/11 Evolution of an Australian National Security Community," 1–20; Baldino and Crawley, *Intelligence and the Function of Government*; and Gyngelland Wesley, *Making Australian Foreign Policy*.
2. See Jones discussion of the establishment of the Special Intelligence Bureau in 1916 and the Commonwealth Investigations Branch of the Commonwealth Police (CIB), the later in particular had a political surveillance role against concerns of growing Soviet subversion.
3. The term 'Five Eyes' is a shorthand phrase used by intelligence officials for AUS/CAN/NZ/UK/US that historically has been stamped on intelligence and intelligence documents shared by Australia, Canada, New Zealand United Kingdom and the United States.

[4] Aldrich, *GCHQ The Uncensored Story of Britain's Most Secret Intelligence Agency*, 89–104; and Herman, *Intelligence Power in Peace and War*. The UKUSA Treaty was amended and modified several times between 1948 and 1956. Australia and New Zealand did not become full members until 1956. See, Pfluke, "A History of the Five Eyes Alliance: Possibility for Reform and Additions," 304.

[5] Horner, *The Spy Catchers: The Official History of ASIO 1949–1963 (Vol. 1)*; Blaxland, & Crawley, *The Secret Cold War, The Official History of ASIO 1975–1989 (Vol. 3)*; Blaxland, *The Protest Years: The Official History of ASIO: 1963–1975 (Vol. 2)*.

[6] The Australian Secret Intelligence Service (ASIS) is Australia's overseas secret intelligence collection agency.

[7] The Australian Signals Directorate (ASD) is the Australian government agency responsible for foreign signals intelligence, support to military operations, cyber warfare, and information security.

[8] Hope, Report of the Royal Commission on Intelligence and Security (3rd Report), 93.

[9] *Ibid*, 3. For background on the significant role played by Justice Hope in shaping the AIC over several decades see, Edwards, Law, *Politics and Intelligence: A Life of Robert Hope*.

[10] Hope, *Inquiry into Security and Intelligence Agencies*.

[11] The original variation of the current Committee the Parliamentary Joint Committee on the Australian Security Intelligence Organisation (the ASIO Committee) was established in August 1988. Following the passage of the Intelligence Services Act 2001, the former ASIO Committee was replaced by the Parliamentary Joint Committee on ASIO, ASIS and DSD (PJCAAD). The legislative basis of the Committee was now in the Intelligence Services Act 2001 (the IS Act) and the PJCAAD met for the first time in March 2002, at the beginning of the 40th Parliament. In 2004 the Committee became the PJCIS.

[12] Jones, and Smith. "Ideology, Networks, and Political Religion: Structure and Agency in Jemaah Islamiyah's Small World," 71–91. This point was also officially acknowledged in the 2004 Flood Report. *Report of the Inquiry into Australian Intelligence Agencies*, 37–41.

[13] Both of these sources provide detailed discussions of CT polices during this period. *Review of Australia's Counter Terrorism Machinery*; Jones, "Intelligence and the Management of National Security: The Post 9/11 Evolution of an Australian National Security Community."

[14] This increase was not entirely for terrorism, new funding was also made available to deal with the surge at the time of maritime people smuggling from the Middle East to Australia via Indonesia. *AFP Annual Report, 2002–2003*, 16.

[15] Department of Foreign Affairs and Trade. *Transnational Terrorism: The Threat to Australia*.

[16] Flood, *Report of the Inquiry into Australian Intelligence Agencies.*

[17] *Ibid*, 83.

[18] Smith, *Summary and Conclusion. Report of the Review of Homeland and Border Security*.

[19] Rudd, *The First National Security Statement to the Parliament*, 4 December 2008.

[20] The National Threat Assessment Centre (NTAC) was established in 2003 and located in ASIO. It provides a 24-hour assessment of threats particularly CT related ones. Its equivalent in the US is the NCTC. Walsh, "Intelligence and National Security Issues in Policing," 109–127.

[21] For example, amendments to Part III of the original 1979 ASIO Act allowed ASIO officers to detain and question persons not yet formally charged of a terrorism offence for a period of 24 hours when this could substantially assist in the collection of intelligence that is important in relation to a terrorism offence. Additionally, a person could be detained up to one week for questioning if there were reasonable grounds he or she may alert another person about an ASIO investigation, was a risk of not appearing for questioning, or could obstruct or destroy material that might be requested under warrant. These amendments proved controversial, with legal and human rights scholars claiming them to be potentially unconstitutional. For a comprehensive review of key pieces of Australian counter-terrorism legislation, struck within the first decade post 9/11 see Williams, "A Decade of Australian Anti-Terror Laws.'

[22] For a discussion of differences between Australian and Canadian counter-terrorism legislation see Walsh "Security Intelligence Collection Since 9/11: Policy and Legislative Challenges, 51–74.

[23] Ibid.

[24] Dempster, "Data Retention and the End of Australian's Privacy," *Sydney Morning Herald*, 28 August 2015.

[25] Walsh and Miller, "Rethinking Five Eyes' Security Intelligence Collection Policies and Practice Post Snowden," 345–367.

[26] Walsh, *Intelligence and Intelligence Analysis*, 210–8.

[27] Walsh and Miller, "Rethinking Five Eyes' Security Intelligence Collection Policies and Practice Post Snowden," 361.

[28] Clarke Report, VII; Walsh, *Intelligence and Intelligence Analysis*, 219–220.

[29] Ibid., X.

[30] Ibid., XI–XII.

[31] Street et al., *Review*, IV.

32. The Rudd/Gillard/Rudd Labor governments enacted efficiency dividends on most AIC agencies, but these were later reduced by the incoming Abbott conservative government. Maley, "Austerity for Spies a Disgrace says Labor MP Anthony Byrne."
33. *Review of Australia's Counter Terrorism Machinery*, 5.
34. *ASIO Annual Report (2017–18*), 7.
35. See note 33 above.
36. Ibid., 10.
37. For example, Fahad Jabhar's assassination of police accountant Curtis Cheng in Parramatta in October 2015.
38. For a good summary of SOCMINT advantages and challenges see, Omand, Bartlett, and Miller, "Introducing Social Media Intelligence (SOCMINT)," 804–6. In the AIC, social media intelligence is conducted in multiple agencies, but the ONI is meant to have a leading role in its collection and analysis.
39. Cornall and Black, *Independent Review of the Intelligence Community Report*.
40. The review was carried out between November 2016 to June 2017. The reviewers engaged in 150 meetings with AIC agencies and other 'Five Eyes' country officials. The review also included 34 submissions from AIC and other government agencies, and from the public see, Walsh, *Submission to 2017 Independent Intelligence Review*, 2016.
41. Ibid., 5.
42. Ibid., 7.
43. Ibid.
44. Ibid., 21–2.
45. Ibid., 18–9.
46. Though the financial impact of COVID-19 on the federal government's budgetary position may impact on how fast ONI can recruit additional staff in the 2020–23 period.
47. DHA, *Annual Report 2017–18*, 12.
48. *Review of Australia's Counter Terrorism Machinery*, 26.
49. DHA, *Annual Report (2018–19)*, 5.
50. The Richardson Review is more formally known as the Comprehensive Review of the Legal Framework Governing the NIC (the Richardson Review).
51. IGIS, *Corporate Plan 2019–20*, 9–10.
52. Walsh, *Submission to 2017 Independent Intelligence Review*.
53. *Independent Intelligence Review*, 123.
54. Ibid., 124.
55. Ibid.
56. Ibid., 5.
57. Walsh, "Improving 'Five Eyes" Health Security Intelligence Capabilities: Leadership and Governance Challenges," 586–602.
58. This point was made by a report commissioned by ONI and peer-reviewed by the author and Sujeeta Bhat from the US National Academies of Sciences, Engineering and Medicine see Withers, *Social Science Research and Intelligence in Australia*.

Bibliography

AFP. *AFP Annual Report (2002–2003)*. Canberra.

Aldrich, R. *GCHQ the Uncensored Story of Britain's Most Secret Intelligence Agency*. London: Harper Press, 2010.

Andrews, C. *The Secret World*. UK: Allen Lane, 2018.

ASIO. *Annual Report (2017-18*). Canberra: Commonwealth of Australia, 2017.

Australian Government. *Review of Australia's Counter-Terrorism Machinery*. Canberra: Department of Prime Minister and Cabinet, 2015.

Baldino, D., and R. Crawley. *Intelligence and the Function of Government*. Melbourne: Melbourne University Press, 2018.

Ball, D., and D. Horner. *Breaking the Codes Australia's KGB Network 1944–1950*. Sydney: Allen & Unwin, 1998.

Blaxland, J. *The Protest Years: The Official History of ASIO: 1963–1975*. Vol. 2. Sydney: Allen and Unwin, 2015.

Blaxland, J. "The New Department of Home Affairs Is Unnecessary and Seems to Be More about Politics than Reform," *The Conversation*, July 19, 2016.

Blaxland, J., and R. Crawley. *The Secret Cold War, the Official History of ASIO 1975–1989*. Vol. 3. Sydney: Allen and Unwin, 2017.

Clarke, J. *The Report of the Clarke Inquiry into the Haneef Case*. Canberra: Commonwealth of Australia, 2008.

Cornall, A., and R. Black. *Independent Review of the Intelligence Community Report*. Canberra: Commonwealth of Australia, 2011.

Dempster, Q. "Data Retention and the End of Australian's Privacy." *Sydney Morning Herald*, August 28, 2015. https://www.smh.com.au/technology/data-retention-and-the-end-of-australians-digital-privacy-20150827-gj96kq.html

Department of Foreign Affairs and Trade. *Transnational Terrorism: The Threat to Australia*. Canberra: AGPS, 2004.

Department of Home Affairs. *Annual Report 2017–2018*. Canberra: Commonwealth of Australia, 2017.

Department of Home Affairs. *Annual Report 2018–2019*. Canberra: Commonwealth of Australia, 2018.

Edwards, P. *Law, Politics and Intelligence: A Life of Robert Hope*. Sydney: NewSouth, 2020.

Flood, P. *Report of the Inquiry into the Australian Intelligence Agencies*. Canberra: Commonwealth of Australia, 2004.

Gentry, J. "Has the ODNI Improved U.S. Intelligence Analysis?" *International Journal of Intelligence and Counterintelligence* 28, no. 4 (2015): 637–661. doi:10.1080/08850607.2015.1050937.

Gyngell, A., and M. Wesley. *Making Australian Foreign Policy*. Cambridge: Cambridge University Press, 2003.

Herman, M. *Intelligence Power in Peace and War*. Cambridge University Press: Cambridge, England, 1996.

Hope, R. M. *Report of the Royal Commission on Intelligence and Security (3rd Report)*. Canberra: AGPS, 1976.

Hope, R. M. *Inquiry into Security and Intelligence Agencies*. AGPS: Canberra, 1984.

Horner., D. *The Spy Catchers: The Official History of ASIO 1949–1963*. Vol. 1. Sydney: Allen and Unwin, 2014.

IGIS. *Corporate Plan 2019–2020*. Canberra.

Johnson, L. "A Conversation with James R Clapper Jr: The Director of National Intelligence in the United States." *Intelligence and National Security* 30, no. 1 (2014): 1–25.

Jones, D. "Intelligence and the Management of National Security: The Post 9/11 Evolution of an Australian National Security Community." *Intelligence and National Security* 33, no. 1 (2018): 1–20. doi:10.1080/02684527.2016.1259796.

Jones, D. M., and M. L. R. Smith. "Ideology, Networks, and Political Religion: Structure and Agency in Jemaah Islamiyah's Small World." *Politics Religion and Ideology* 13, no. 4 (2012): 71–91. doi:10.1080/21567689.2012.725664.

Kitney, G. "Politics and Policy Meet in New Home Affairs Department." *The Interpreter*, 2017

L'Estrange, M., and S. Merchant. *Independent Intelligence Review*. Canberra: Commonwealth of Australia, 2017.

Maley, P. "Austerity for Spies a Disgrace Says Labor MP Anthony Byrne." *The Australian*. May 28, 2013.

Omand, D., J. Bartlett, and C. Miller. "Introducing Social Media Intelligence (SOCMINT)." *Intelligence and National Security* 27, no. 6 (2012): 801–823. doi:10.1080/02684527.2012.716965.

Pfluke, C. "A History of the Five Eyes Alliance: Possibility for Reform and Additions." *Comparative Strategy* 38, no. 4 (2019): 302–315. doi:10.1080/01495933.2019.1633186.

Rudd, K. *The First National Security Statement to the Parliament*. Canberra: Commonwealth of Australia, December 4, 2008. http://www.pm.gov.au/media/speech_0659cfm

Smith, R. *Summary and Conclusion. Report of the Review of Homeland and Border Security*. Canberra: Commonwealth of Australia, December 2008.

Street, S. L., M. Brady, and K. Moroney. *The Street Review of the Interoperability Between the Australian Federal Police and its National Security Partners*. Canberra: Commonwealth of Australia, 2008. http://apo.org.au/resource/streetreview.

Walsh, P. F. *Intelligence and Intelligence Analysis*. Abingdon: Routledge, 2011.

Walsh, P. F. "Intelligence and National Security Issues in Policing." In *Policing in Practice*, edited by P. Birch and V. Herrington, 109–127. Sydney: Palgrave Macmillan, 2011.

Walsh, P. F. "Building Better Intelligence through Effective Governance." *International Journal of Intelligence and Counterintelligence* 28, no. 1 (2015): 123–142. doi:10.1080/08850607.2014.924816.

Walsh, P. F. "Security Intelligence Collection since 9/11: Policy and Legislative Challenges." In *National Security, Surveillance, and Terror: Canada and Australia in Comparative Research*, edited by R. Lippert, K. Walby, and D. Palmer, 51–74. Cham, Switzerland: Palgrave Macmillan, 2016.

Walsh, P. F. "Submission to 2017 Independent Intelligence Review." Submission to Government Report, 2016.

Walsh, P. F. *Intelligence, Biosecurity and Bioterrorism*. London: Palgrave Macmillan, 2018.

Walsh, P. F. "Improving 'Five Eyes' Health Security Intelligence Capabilities: Leadership and Governance Challenges. Intelligence and National Security." *Intelligence and National Security* 35, no. 4 (2020): 586–602. doi:10.1080/02684527.2020.1750156.

Walsh, P. F., and S. Miller. "Rethinking Five Eyes Security Intelligence Collection Policies and Practice Post Snowden." *Intelligence and National Security* 31, no. 3 (2016): 345–368.

Williams, G. "A Decade of Australian Anti-Terror Laws." *Melbourne University Law Review* 35, no. 3 (2011): 1137–1151.

Withers, G., E. Buchanan, L. West, D. Clements, and G. Austin. *Social Science Research and Intelligence in Australia*. Canberra: Australian Academy of Social Sciences, 2019.