Paper for Presentation at the ISA, 60th Annual Convention, Toronto (27th March 2019)

Transforming the Australian Intelligence Community: Mapping Change, Impact and Governance Challenges

Patrick F Walsh (Charles Sturt University, Australia)

Abstract

9/11 produced significant changes to the US intelligence community, while for the most part the attacks only resulted in incremental 'tinkering' or evolutionary change of the Australian intelligence community (AIC). Fast forward to 2017 however, a combination of variables, including most importantly a recent independent intelligence review of the AIC is ushering in potentially transformative change to the Community. This paper examines how the 2017 Independent Intelligence Review has created the momentum for significant change in the AIC and what governance challenges are likely to result from reform initiatives flowing from the Review. The paper also investigates whether the current AIC reform agenda is truly transformative and if it is also likely to result in a more effective, coordinated and integrated intelligence community.

Key words: Australian intelligence community, Independent Intelligence Review 2017, Five Eyes alliance, intelligence governance.

Introduction

This paper explores how the 2017 Independent Intelligence Review is currently setting the agenda for major reform of Australia's Intelligence Community (AIC). It investigates what were the Review's key recommendations and how these are being translated in the reform agenda. In particular, the paper asks two questions: is the reform agenda now underway transformational and is it likely to yield a more effective, coordinated and integrated

Community? Before exploring both questions, it is necessary first to place the current reform agenda into its historical context.

Historical context

This first section, provides a brief historical context of key milestones in the AIC's development. The objective is not to provide a detailed history of all changes in the AIC leading up to 2017. However, in order to understand contextually the contemporary reform agenda, the paper provides a brief analysis of key historical landmark events, issues and policies from 1945 up to 2017. The analysis shows that except at a few points in time, the AIC's development has been largely incremental or evolutionary in nature compared to the contemporary changes now underway.

Cold War to September 11 2001 (1500)

Starting a brief historical overview of the AIC at 1945 may seem a bit 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. Similar to later developments after World War 2, the establishment of at least a rudimentary intelligence capability in Australia was due initially to UK then US national interests and concerns over Japanese regional influence and then Soviet influence within Australia. As Jones, notes it was 'at the behest of the British Counter Espionage Service the Australian Commonwealth established its first Special Intelligence Bureau in 1916.'[1] Additionally, the fear of communist subversion in the inter war period and after 1945 resulted in the Commonwealth Investigation Branch of the Commonwealth Police (CIB) assuming responsibility for political surveillance.

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 US and UK) were to have significant influence on its development. Several historical accounts underscore the important implications that arose from the United States and

its Anglosphere partners being victors in World War 2. Such 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 in 1948, which has deepened significantly since.[2]

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. 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.[3] 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. DSB was later renamed the Defence Signals Directorate (DSD) in 1978, and most recently the Australian Signals Directorate-ASD in 2013. The rationale for the last name change in part was a desire by government to highlight

that ASD although in the defence portfolio has 'whole of government' responsibilities beyond just military priorities.

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 were derivative products (ASD, DIO and AGO) of the Cold War, and responded to suspicions of Soviet espionage in the Asia Pacific at the end of the Second World War and the KGB's penetration of Australia's federal government revealed by the Venona transcripts.[4]

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 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.[5] Arguably, the 1977 Hope Royal Commission was the greatest catalyst for change within the AIC up to 9/11 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.'[6] To remedy this, the Liberal government of Malcolm Fraser 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.[7] 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. 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. The Hope Royal Commissions produced significant change in the coordination and accountability mechanisms in the AIC. In a sense both inquiries 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. The Cold War was a challenging period for all 'Five Eyes' partners, but 'the core intelligence task – the monitoring of the USSR's strategic and military posture – remained within predictably limited bounds.'[8] The post Hope Royal Commission AIC seemed to lend

itself to this single core task negating at least in the minds of successive Australian governments the need for any wholesale rethink of its structure.

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 actors threats were now vying for the attention of successive Labour 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 Philippine 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.[9]

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.[10] 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.[11] 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.[12] 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. Other MOUs on counter-terrorism cooperation were later signed across the Asia-Pacific during 2002 to 2010. During this period, the increased policy focus on counter-terrorism by successive Australian governments also facilitated greater intelligence collection efforts across the AIC. In particular, Canberra's participation in the invasion of Afghanistan in 2002 and Iraq in 2003 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, 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.[13] The latter and additional focus would have provided a more comprehensive review. Flood made 23 recommendations. Many of these concerned improving analytical contestability and strengthening oversight as well as increasing ONA's meagre budget. In the main though, Flood concluded that the architecture designed by Justice Hope in the 1970s for the Australian intelligence community remained valid, and there was no need for fundamental structural change.'[14] Notably though, Flood did recommend another review of the AIC in a period of 5

to 7 years and since 2004 governments of both political persuasion have commissioned two additional independent inquiries into the AIC. The next occurred under the Gillard Labour government in 2013 and the third occurred in 2017 under the Turnbull liberal coalition government. The significance of latter will be discussed shortly.

While the Flood Report underscored no significant change to the AIC's basic architecture, its overall capability was nonetheless enhanced from 2004 onwards with increased funding and a proliferation of legislation that allowed more flexible and proactive intelligence collection, disruption and prosecution of terrorist offenders.

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 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 US 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.[15]

In the end the Smith Review, discounted the need for a US 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 in 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.'[16] Other minor

structural change to the AIC saw the establishment in 2011 of Counter-Terrorism Control Centre (CTCC) housed in ASIO to overcome some of siloing of information seen in National Threat Assessment Centre and promote more efficient identification of intelligence and investigative priorities.[17]

Rudd also begun promulgating an expanded version of the AIC to underpin his broader definition of national security. The AIC started to be referred to as 'the National Intelligence Community' to signify a more 'whole of government' approach to national security that went beyond traditional threats to those normally viewed as part of the human security agenda such as climate change and pandemics. As noted earlier, legislative activism and increased funding were the two main themes driving any AIC reform from 9/11 to the mid-2000s. We now turn our attention to how legislation and funding impacted on the AIC from the mid-2000s to 2017.

In the first decade after 9/11, 54 pieces of anti-terrorism legislation was passed by the federal parliament and many of these increased the powers of AIC agencies such as ASIO to and AFP to hold and question suspects for longer periods before being charged and to control the movements of others.[18] 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 nonetheless the net effect from 2001 to 2011 in particular, was successive Australian governments were much more prolific in passing several large pieces of counter-terrorism and intelligence related legislation compared to other 'Five Eyes' partners.[19]

As the threat from terrorism offshore and in Australia evolved 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. The legislation was designed to manage a newer unfolding threat trajectory– of young Muslim Australians seeking to go to

Syria and fight for the IS Caliphate. The consolidation of the Caliphate saw a parallel rise in concern by the Abbott government of Muslim youth from western Sydney and Melbourne suburbs being recruited to fight for IS. In 2014, and in order to deter would be foreign fighters, the government passed *The Counter Terrorism Legislation Amendment (Foreign Fighters) Act (2014)* to prevent Australians suspected of being radicalised jihadists travelling to proscribed areas of concern in the Middle East. At the same time, two other major pieces of legislation – *the National Security Legislation Amendment Act (2014),* and *the Telecommunications (Interception and Access) Amendment (Data Retention) Act (2014)* were also enacted. 'Although each piece of legislation has been aimed at slightly different objectives they all represented a significant enhancement of Australia's national security and intelligence collection capabilities–arguably not seen since the Howard Government in 2007.'[20]

These acts however, were the latest examples of a narrative running since the Howard Government that the AIC needed even more proactive intelligence collection capabilities as terrorist threat evolved.[21] In practice, they represented greater powers granted across all intelligence agencies, including ASIO, the AFP, the Australian Signals Directorate (ASD) and the Australian Secret Intelligence Service (ASIS).'[22] The data retention amendments to the Telecommunications (Interceptions and Access) Act were argued as being urgently required by the AIC and the government to address both recruitment of IS and to provide more warning against lone actor attacks that were starting to occur in Sydney and Melbourne.[23]

Yet at this time, an accumulation of over 15 years of either amended or new counter-terrorism and intelligence legislation began 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 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 Australian intelligence community was spying on senior members of the Indonesian government including on behalf of the NSA during US-Indonesian trade talks.[27] Since the recent tranche of counter-terrorism laws other states such as the US during the Obama Administration have stepped back from some of the proactive and privacy concerning measures represented in the Australian legislation.[28]

In summary, 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 appropriately used, proportionate or legal. But the seeds of growing community concerns were already in place by the mid-2000s. The AFP's detention and arrest of Dr Mohamed Haneef for his alleged role in failed attacks on a London nightclub and Glasgow airport in July 2007 in particular fuelled debates about how new powerful counter-terrorism laws were being operationalised by AIC agencies. AFP officers arrested Haneef at Brisbane airport in July 2007 in connection with a failed terrorist attack on Glasgow International Airport that involved his second cousins Kafeel and Sabeel Ahmed. He was held in solitary confinement for 12 days under the Anti-Terrorism Act 2005, but was eventually released without charge.

The subsequent inquiry into the Haneef case led by former New South Wales Justice John Clarke QC 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.'[29] Ultimately, Clarke concluded that AFP Commander, Ramzi Jabhar, 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.'[30] Clarke recommended parliament implement

oversight of the AFP and reform the counter-terror legislation.[31] 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'[32] This deficiency stemmed from three sources: firstly, the conflict between the intelligence-gathering function of the security agencies and the evidence gathering of police; secondly, the problem of confidentiality in terms of intelligence-gathering versus the constitutional requirement of accountability; and thirdly the tendency of different security agencies to 'silo' information. This third point had been previously identified in the 2004 Flood Report into the Australian intelligence agencies.

In addition to the enactment of a large volume of counter-terrorism and intelligence related legislation, from the mid 2000 onwards governments of both political parties (Labor and Liberal) continued to invest heavily in AIC agencies head count, budgets as well as sponsoring other fusion arrangements to promote intelligence priority setting, collection and sharing amongst agencies working on counter-terrorism.[33]

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.[34] 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.[35] By the close of the decade, whilst the Flood Report called for a doubling of ONA analysts, staff projections are expected to be around 300 over the next two years. 'ASIS, which does not disclose staff numbers, saw its budget rise from $36 million in 2003 to nearly $250 million a decade later'. 'Over a similar period, the Australian Federal Police, which had assumed an enhanced counter terrorism function after 2002, saw its

personnel increase tenfold from 647 to 6400 officers'.[36] Although the level of AIC funding fell a little after the Labor government's review of counter-terrorism in 2008, mounting concern about the internal and external threat posed by the rise of Islamic State saw Tony Abbott's Liberal government increase the AIC budget by a further AUD $634 million in 2014.[37] 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 Liberal (conservative) Government was based by an assessment by cabinet that the threat from global Islamist terrorism was growing and becoming even more diverse and complex.[38] 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.[39] 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.[40]

The emergence of Islamic State in 2014 and the 'lone actor attacks' in Melbourne and Sydney discussed earlier coincided with Tony Abbott's new Liberal 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 and 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, however, 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.[41] 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. Little detail was given at that time, but like the 2011 review the language of the media statement implied a 'health check' rather than the patient was sick and needed immediate invasive surgery. In short, unlike the Flood Report no pressing intelligence failure needed investigating, but unlike the two earlier AIC reviews into the AIC, the 2017 version proved to be more comprehensive in reaching out to AIC agencies, political leaders, other AIC customers and the community for consultation.[42] Given limited space, the following section, focuses on the most critical of the review's 23 recommendations, particularly those that relate to a final discussion below on whether these amount to a structural transformation of the AIC not seen since 40 years ago following the two commissions into the intelligence community by Mr Justice Hope in 1970s and 1980s.[43]

The 2017 Independent Intelligence Review

The most important recommendation (number 1) was that that an Office of National Intelligence (ONI) be established as a statutory body within the Prime Minister's portfolio. This Office would be headed by a Director-General, who 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 direct the co-ordination of the national intelligence community to ensure there are appropriately integrated strategies across the suite of agency capabilities.

ONI would also be given the responsibility for enterprise-level management of the national intelligence community, 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.'[44] 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.[45]

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 facilitating closer coordination, evaluation and integration of cyber security and counter-terrorism intelligence. Although the former ONA has played a central role in the coordination of various AIC intelligence activities, adding formally an integration and evaluation function signalled an expectation by government that ONI was to have a more formalised role in how the AIC as a whole was working and reporting this back to government regularly. The third most important recommendation (number 13) suggests that ONI should become responsible for leading and co-ordinating data management and ICT connectivity initiatives across the National Intelligence Community. This make sense and is similar to the role the US ODNI has tried to take on in building a single IT enterprise across the community or what has become known as ICITE (Information Technology Enterprise of the Future).[46]

Fourthly, there were four recommendations that dealt with various oversight and accountability matters. The first two related to a comprehensive review of Acts governing the AIC (recommendation 15); an expansion of the oversight role of the Parliamentary Joint Committee on Intelligence and Security; and the expansion in the number of oversight Inspector-General of Intelligence and Security (IGIS) to apply to ten agencies within the National Intelligence Community. This long overdue expansion of IGIS's remit means it now has oversight of the intelligence functions of Australian Federal Police, the Department of Immigration and Border Protection, and the Australian Criminal Intelligence Commission. 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 of IGIS to at least 50– allowing more frequent and deeper inspections of AIC operations.[47] 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 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 ten 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 on the AIC. Two remedies were identified. One was 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.[48] The reviewers suggested that a National Intelligence Community Innovation Hub could be a way to bring together government, industry and academia to address capability gaps and create new linkages. 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.

Operationalising review recommendations

The government accepted all the recommendations of the Review upon its release in June 2017. The most important of these 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 head count is expected to roughly triple to about

300 staff over the next few years. ONI's head count is 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. ONI is moving to fulfil its new legally mandated functions though a new building is still under construction and more staff need to be hired to begin to operationalising many of the Review's recommendations.

Recommendation 3 as discussed earlier which has given the ONI overall responsibility for enterprise-level management of the national intelligence community is also being implemented– though as discussed below these processes will take longer to bed down.

Additionally, there were four Review recommendations that dealt with various oversight and accountability matters, where some progress has made towards their implementation. For example, recommendation 15 called for a comprehensive review of Acts governing the AIC. This commenced in May 2018 following a 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. Mr Richardson will release a secret report followed by an unclassified version in late 2019.

The other aspects of this recommendation (no 15); an expansion of the oversight role of the Parliamentary Joint Committee on Intelligence and Security and the Inspector-General of Intelligence and Security be expanded to apply to all ten agencies within the National Intelligence Community are sensible reviews, but at the time of writing it's unclear whether the IGIS Act has been amended. 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. Advising the government to increase full time staff to at least 50 should allow more frequent and comprehensive inspections of AIC operations by the Office of Inspector-General of Intelligence and Security. Similarly the expanded oversight role for the

Parliamentary Joint Committee (PJCIS), where it will now be able to request IGIS to conduct an inquiry into the legality and propriety of operational activities and provisions and for the Committee to initiate its inquiries into the administration and expenditure of the now ten intelligence agencies is a significant change. But at the time of writing the government has not made amendments to the Intelligence Services Act 2001 Part 4 (29) which outlines the functions of the Committee's powers.

The final recommendation (no 14) that is noteworthy, is the suggestion by Reviewers that ONI needed a more structured and strategic approach to identifying the impact of changes in science and technology to the AIC. Two remedies were identified. One was 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. Given though, ONI is still establishing and appointing staff in key positions (both in assessments and enterprise management groups), the establishment of both the National Intelligence Community Science and Technology Advisory Board, the National Intelligence Community Innovation Hub and the national community innovation funding are likely yet to be established.

Outlook

As discussed the many Review recommendations currently being implemented in the AIC – particularly the establishment of the ONI represent collectively the most significant changes to the structure of the AIC since those put in place after Mr Justice Hope 40 years ago. The growing complexity in the security environment–including the blurring of foreign and domestic threats and malevolent use of technology by threat actors (both state and non-nation state)– underscored the need for a third review of AIC's structure to determine whether it is fit for purpose now and into the future. The Review, overwhelmingly endorsed an AIC that was

performing well against this complex security environment. However, at the same time the Reviewers argued that its structure could be improved upon to allow the AIC to function not just as a collection of agencies, but as confederated intelligence enterprise where resources, priorities and strategic planning are more effectively coordinated.

While the Review has provided the catalyst for significant structural reform in the AIC, in this final section, the paper addresses two key questions. First, do the key Review recommendations outlined earlier represent transformational change in the AIC–in the mould of those reforms seen after the Hope Royal Commissions? Second, will post Review reforms fundamentally drive a more effective, sustainable and adaptive AIC; or will the individual histories of intelligence agencies, bureaucratic culture, politics or funding constrain the potential significance of the post Review AIC reform now underway? What are the prospects that from 2019 to 2025–(the later date being when the likely (fourth) independent intelligence review will occur) that the 2017 Review reforms will have produced an even more responsive AIC that potentially is seen as world class amongst other Five Eyes partners and allies?

Regarding the first question, it's clear that post Review reforms now being implemented are significant though they are not yet transformational. If 'significant' is taken to mean *important reforms* with the *potential for change* and 'transformation' is meant to convey *radical change* or a *process that changes the underlying structure* –then it is far too early in the implementation of post Review reforms to argue the case current changes are transformational. ONI whose responsibility is to shoulder much of the AIC reform has legally only been in existence since December 2018. At the time of writing (March 2019), ONI is still hiring sufficient staff and expanding its offices in anticipation of implementing its reform mission. Whether the combined anticipated reforms will be transformational therefore, will require more time to

assess. Most probably another five years at least would be a reasonable amount of time for an early estimation of whether various reform measures have got traction both in ONI and the broader AIC. But in reality it may take decades as it did for the Justice Hope post AIC reforms to provide any clear assessment on whether reforms amount to just another suite of bureaucratic reforms or a fundamental shift in how the AIC enterprise operates. It will be also difficult for external researchers to make a comprehensive assessment on whether reforms have resulted in transformational change to the AIC given the closed nature of the Community. Nonetheless, it is likely some tentative judgments may be possible over time as oversight bodies such as the IGIS and the PJCIS report on aspects of AIC operations.

The second question relates to whether the post Review reforms will fundamentally drive a more effective, sustainable and adaptive AIC. Change can be significant or transformational, but it can result in less effective intelligence governance and capability. This second question is also difficult to assess given the implementation of many post Review recommendations remain in progress. In essence, the effectiveness of most of the reform measures currently in the pipeline will rest on how well the new ONI is able to assume its legal and bureaucratic mandate for intelligence governance across the AIC.[49] The main theme in the Report was the importance of a single point of coordination for the AIC. The Reviewers argued that a single point of coordination was not as clear in the AIC as other 'Five Eyes' partners such as the UK and USA. They said: 'it is notable that both the United States and the United Kingdom took steps after the attacks of 11 September 2001 and 7 July 2005 respectively to strengthen the co-ordination and integration of their intelligence communities.' 'They have continued to do so in the intervening period and the result in both countries is strong, strategic-level management of intelligence as a national enterprise built on the specific attributes of individual agencies'. This

has enhanced both effectiveness and efficiency, even against the tragic backdrop of terrorist attacks over recent year's economic, societal and technological changes.'[50]

The general point the reviewers make about improvements in central coordination of other 'Five Eyes' ICs is reasonable enough, yet research highlights that there is no 'silver bullet' to designing the 'right kind of structure' that results in an effective, central point of coordination and integration. There are scholars and former IC staff in the US, who still critique the ODNI's ability to live up to its mandate to be an effective central point of coordination and integration for the US IC.[51] The ONI which is in the driving seat for most post Review reform will need to learn the lessons of how ODNI and other centralised intelligence coordination arrangements in the UK, Canada and New Zealand have been challenged by making their IC enterprises greater than the sum of its parts. It will be as important to learn the bad as much as the good lessons from other 'Five Eyes' partners. With a new legal mandate and increased resources ONI will need to take its time to get the balance right between respecting individual agency mandates and cultures while forging a stronger collective AIC identity that promotes better coordination, integration and mutual development of capability.

Getting this balance right between respecting individual agency identity and forging a common identity and mission will remain a work in progress for the foreseeable future. As noted earlier, the individual histories of intelligence agencies, bureaucratic cultures, politics and budgets are just some of the variables that will constrain the success ONI will have it is newly expanded intelligence, coordination, integration and engagement roles. Of particular importance will be some early wins for ONI, particularly in its newly appointed Deputy Director General Intelligence Enterprise Management portfolio. While the Review has already resulted in greater integration particularly on the cyber front with the co-location of all relevant AIC agencies in

the Australian Cyber Security Centre– the Reviewers did not explicitly make clear whether they had intended for the D/DG Intelligence Enterprise Management position to take on a wider intelligence governance mandate across a suite of national intelligence priorities including emerging ones.

There are a number of technologically enabled threats that are not on the AIC's radar such threat actors weaponising synthetic biology and biotechnology that the ONI with its new enterprise management role could bring about better governance over collection and assessment capabilities.[52] There is still likely much to be resolved amongst AIC agencies in more conventional threat spaces such as counter terrorism as ONI takes on greater authority over the setting of intelligence priorities and the evaluation of various agencies against them. For example as noted earlier, ASIO has played a leading role within the National Threat Assessment Centre (NTAC). The CCTC also sets priorities and evaluates agencies performance against these counter-terrorism priorities. Both coordinating and fused bodies seem to working adequately, yet the Reviewers recommended that a senior dedicated ONI position be appointed to facilitate closer coordination and integration across the national counter-terrorism intelligence effort. It is likely there will be a need for greater de-confliction and clarification of coordination roles between ONI and other AIC agencies, who have historically held similar functions and responsibilities.

More significantly though de-confliction in coordination and integration of intelligence activities will also need to occur not just within the AIC agencies, but between it and the recently established Department of Home Affairs (DHA). The Department of Home Affairs was created by the Liberal 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.[53]

Each of the six participating agencies maintain their statutory independence. 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.'[54]

It's 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 previously three or four invest a single minister with enormous power.[55] Others have more

cynically suggested that the ministry was created by the now deposed former Prime Minister Malcolm Turnbull to reward its newly appointed minister Peter Dutton for being a bulwark between the Prime Minister's moderate party faction and another right wing faction that was agitating for deposing Turnbull. Dutton himself was part of that right wing faction and Turnbull's appeasement to Dutton in creating DHA was ultimately unsuccessful as Turnbull was later replaced as prime minister on 24th August 2018.[56] While senior members of the intelligence and law enforcement community have not engaged in public debates about the rationale for the establishment of the DHA, it's clear that many held the view that the government was fixing something that wasn't broken. Indeed less than two 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.'[57]

In the initial six months after DHA's creation it has demonstrated progress with the establishment of 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. As far as intelligence capability is concerned the official language describing DHA's new intelligence and capability group says its 'role is to provide the department's intelligence services and products to support decision-making, policy development, resource allocation and counter border threats and provide enterprise leadership on major capability projects.'[58] But in reality it is still the individual departments sitting under the DHA that provide intelligence services, and at this point it's unclear how the broader ministry will value add to current intelligence services and capabilities. This may become clearer later but it is not now.

Both ONI and DHA have been given significant capability investments to implement new mandates. There are funds for training, professionalization and likely in the future resources for investing science and technology and research. Given that many of the agencies in the DHA are also part of the ONI, the leadership of both agency will need to work closely together to ensure a strategic and cost-effective way to investing in national intelligence capabilities particularly in research and training. For example, both ONI and DHA have intelligence capability areas for training and individual agencies have their own as well. With the inevitable overlap between ONI and DHA's missions, further reflection is needed on what opportunities their might be for joint ONI-DHA sponsored training and what areas are best left to ONI, DHA or its independent agencies to deliver? This same question is relevant to how ONI and DHA will invest in future intelligence capabilities. What should be done collaboratively and what projects are best left to either departments or the agencies within them?

In addition to how well ONI can take on its newly expanded intelligence governance role of coordination and integration, a more effective, sustainable and adaptive AIC will also rely on how the new agency can implement its expanded evaluation functions. Division 2 Section 7(10(b) lists its evaluation function. Division 2 Section 9 provides more detail of how ONI will take on this evaluation role of the AIC.[59] Unlike the former ONA Act, which focused solely on its charter to evaluate foreign intelligence priorities, the new ONI Act gives it powers to evaluate national intelligence priorities and the intelligence needs of ministers.[60] This new provision in the ONI Act suggests a blurring between what was once considered national security (or security intelligence) and foreign intelligence. It's unclear in practice how ONI will operationalise the intent expressed in the Act to evaluate foreign vs national intelligence. Clause 9(1) (b) also provides further details about its new role in evaluating whether AIC resources are adequate and being allocated appropriately.[61] Again a welcome provision in the

new Act, yet unclear is what metrics will be used to evaluate whether AIC resources are adequate or being allocated appropriately. The later metric lends itself potentially to internal bureaucratic bias about what is the 'appropriate use of resources.' Finally, (Clause 9(1)(d) also allows the Prime Minister to direct ONI to evaluate an agency or agencies to assess the AICs effectiveness in relation to specific matters such as an intelligence failure. This seems like a useful provision in the Act, but again its unclear how in practice ONI's more formalised evaluations of other AIC agencies will occur. In the case of any significant intelligence failure, ONI may be able to provide the government with a quick classified version of factors that led to an attack against Australia's interests or agency underperformance. Though any internal evaluation of intelligence failure by ONI would need to be augmented by AIC's oversight and accountability mechanisms, particularly the IGIS and PJCIS.

Finally, ONI's leadership role in the AIC suggest it needs to take on greater responsibility in upgrading legacy ICT systems that span across the entire intelligence enterprise including how they can be linked securely but efficiently where needed to lower classified systems. There are less data systems to deal with in the AIC than in US particularly in the inner AIC agencies, though there remain ongoing problems in the storage, sharing particularly with law enforcement agencies also in the AIC. The national AIC law enforcement agencies are also attempting to renovate their systems so there will be ongoing governance issues to sort out so systems can integrate more easily at the appropriate security classification levels.

While ONI has been in existence only since December 2018 progress is being made. Yet realistically it will likely to take a 3-5 more years until discernible improvements can made in many of the major Review recommendations discussed above. At the time of writing, (March 2019) Australia will be going into a national election scheduled for May. While reform processes continue, progress on bigger capability issues such as capability funding, workforce

planning and evaluations may be put on the back burner until senior ONI and AIC leaders have a clearer picture of the new incoming government's perspectives on the current AIC reform agenda. The post Review recommendations combined represent an ambitious reform agenda, but it remains less clear at this point whether they will be either transformational or effective.

Notes

[1] Jones, "Intelligence and the Management of National Security: the Post 9/11 Evolution of an Australian National Security Community,"4.
[2] Aldrich, *GCHQ The Uncensored Story of Britain's Most Secret Intelligence Agency*, 89-104; Herman, *Intelligence Power in Peace and War*, 1996.

[3] The Australian Secret Intelligence Service (ASIS) is Australia's overseas secret intelligence collection agency.
[4] Project Venona represented efforts by US and UK to code break Soviet intelligence and other telegrams. Some 3000 communications were intercepted in the early Cold War period (1939-48), mainly messages exchanged between Moscow and its intelligence residencies in the United States. See, Andrews, *The Secret World*, 672; Ball, Horner. *Breaking the Codes Australia's KGB Network 1944–1950*, 1998.

[5] Hope, *Report of the Royal Commission on Intelligence and Security (3rd Report)*, 1976, 93.
[6] Ibid, 3.
[7] Hope, *Inquiry into Security and Intelligence Agencies*, 1984.
[8] Rathmell, "Towards Post Modern Intelligence," 87-104.
[9] Jones, and Smith. "Ideology, Networks, and Political Religion: Structure and Agency in Jemaah Islamiyah's Small World." 2012, 71–91. This point was also officially acknowledged in the 2004 Flood Report. *Report of the Inquiry into Australian Intelligence Agencies*, July 2004, 37-41.

[10] Both of these sources provide detailed discussions of CT polices during this period. *Review of Australia's Counter Terrorism Machinery,* 2015*;* Jones, "Intelligence and the Management of National Security: the Post 9/11 Evolution of an Australian National Security Community," 2018.
[11] 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.
[12] Department of Foreign Affairs and Trade. *Transnational Terrorism: The Threat to Australia*. Canberra: AGPS, 2004.
[13] Flood, *Report of the Inquiry into Australian Intelligence Agencies*, July 2004.
[14] Ibid, 83.

[15] Ric Smith, *Summary and Conclusion. Report of the Review of Homeland and Border Security*, December 2008.
[16] Rudd, *The First National Security Statement to the Parliament,* December 4, 2008
[17] 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," 2011, 109-127.
[18] 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," 2011.

[19] For a discussion of differences between Australian and Canadian counter-terrorism legislation see Walsh "Security Intelligence Collection Since 9/11: Policy and Legislative Challenges," 2016, 51-74.

[20] Ibid.

[21] Ibid.
[22] Ibid.
[23] Like other Five Eyes and Western allies, there have been an increased number of lone actor attacks in Australia's major cities. In 2014, Abdul Numan Haider attacked two police officers – one AFP and one Victorian Police – outside a police station in Melbourne. Haider stabbed both police officers before being shot dead. On 15 December 2014: Martin Place siege. Man Haron Monis took 17 hostages in a café in Martin Place, Sydney. Two hostages, and Monis, died in the siege. Monis stated his actions were an attack by ISIL in negotiations during the siege. In October 2016, Fahad Jabhar assassinated police accountant Curtis Cheng outside of NSW Police Headquarters. Jabhar had been radicalised by online material.
[24] Dempster, "Data Retention and the End of Australian's Privacy," Sydney Morning Herald, 28th August 2015.
[25] Walsh and Miller, "Rethinking Five Eyes' Security Intelligence Collection Policies and Practice Post Snowden," 2015, 345-367.
[26] Walsh, *Intelligence and Intelligence Analysis*, 2011, 210-218.
[27] Walsh and Miller, "Rethinking Five Eyes' Security Intelligence Collection Policies and Practice Post Snowden," 2015, 361.

[28] Section 215 of the US Patriot Act was continually extended rather than comprehensively reviewed. After the 2013 the Snowden leaks, in June 2015 it was amended following President Obama signing into law the USA Freedom Act (H.R. 2048). The USA Freedom Act reauthorized some expired provisions under Section 215 of the Patriot Act (e.g. the collection of business records in national security investigations), but also prohibited others namely the bulk collection of data of American's telephone and internet metadata by the NSA or other US intelligence agency. Collection must now be linked to by a 'specific selection term (SST) meaning an identifiable person, account, address or personal device not the mere bulk collection of data.
[29] Clarke Report, VII; Walsh, Intelligence and Intelligence Analysis, 219-220.
[30] Ibid, X.
[31] Ibid, XI-XII.
[32] Street et al., *Review*, IV.

[33] The Rudd/Gillard/ Rudd Labor governments enacted efficiency dividends on most of the AIC agencies, but these were later reduced by the incoming Abbott conservative government. Maley, "Austerity for Spies a Disgrace says Labor MP Anthony Byrne."
[34] *Review of Australia's Counter Terrorism Machinery*, 5.
[35] *ASIO Annual Report (2017-18), 7*
[36] Jones, "Intelligence and the Management of National Security: the Post 9/11 Evolution of an Australian National Security Community,"8.
[37]
[38] *Review of Australia's Counter Terrorism Machinery,* 10.
[39] For example, Fahad Jabhar's assassination of police accountant Curtis Cheng in Parramatta in October 2015
[40] For a good summary of SOCMINT advantages and challenges see, Sir David Ormand, Jamie Bartlett and Carl Miller, 'Introducing Social Media Intelligence (SOCMINT)'2012, 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.
[41] Cornall and Black, *Independent Review of the Intelligence Community Report*, Canberra: Commonwealth of Australia, 2011.
[42] The review also included submissions from the public including mine, Walsh, *Submission to 2017 Independent Intelligence Review,* 2016.
[43] L'Estrange, and Merchant, *Independent Intelligence Review*, 2017.
[44] Independent Intelligence Review p. 7
[45] ibid
[46]*Independent Intelligence Review,* 18; Johnson, "A Conversation with James R Clapper Jr: The Director of National Intelligence in the United States," 1-25.
[47] *Independent Intelligence Review*, 21-22
[48] Ibid, 18-19
[49] Intelligence governance is a term I have used in research on IC capability issues since 2011. In the book *Intelligence and Intelligence Analysis,* 131-152, I developed an effective intelligence framework. The framework showed that sound and adaptable IC capability relied on how well both core intelligence processes and key enabling activities worked together to produce intelligence outcomes decision-makers needed. In this research governance was defined as 'attributes and rules pertaining to strong sustainable leadership, doctrine design, evaluation, and effective coordination, cooperation and integration of intelligence processes,'149. In simple terms, governance is about effective leadership and it has an external dimension ('the political leadership') and an internal one (heads of IC agencies and communities). Also see, Walsh, "Building Better Intelligence through Effective Governance." 2015, 123-142
[50] IIA 6-7
[51] Gentry, "Has the US ODNI Improved Intelligence Analysis"? 2015. International Journal of Intelligence and Counterintelligence, 28/4, 2015, 637-661. Problems with ODNI sources
[52] Walsh, *Intelligence, Biosecurity and Bioterrorism*, 2018.
[53] Department of Home Affairs, Annual Report 2017-2018
[54] Ibid, X.
[55] Blaxland, "The New Department of Home Affairs is Unnecessary and Seems to Be More About Politics than Reform, 2016.
[56] Kitney, "Politics and Policy Meet in New Home Affairs Department," 2017
[57] *Review of Australia's Counter Terrorism Machinery,* 26.
[58] *DHA Annual Report*, 2017-18, 18.
[59] *Office of National Intelligence Act 2018*, 10, 12-13.
[60] Ibid.
[61] Ibid.

Disclosure Statement

No potential conflict of interest was reported by the author

Notes on Contributor

Dr Patrick F Walsh, is an Associate Professor (Intelligence and Security Studies) at the Australian Graduate School of Policing and Security, Charles Sturt University, Australia. He is a consultant to government agencies on intelligence reform and capability issues. Prior to academia, he was an intelligence analyst working for a range of Australian Government agencies. He has published several peer reviewed works on intelligence reform issues. His most recent book is: *Intelligence, Biosecurity and Bioterrorism* (London: Palgrave Macmillan, 2018).

ORCID

https://orcid.org/0000-0002-1369-5468

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.

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

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

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*, 28th August, 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.

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

Gentry, J. "Has the US ODNI Improved Intelligence Analysis"? *International Journal of Intelligence and Counterintelligence*, 28/4, 2015, 637-661.

Herman, M. (1996). *Intelligence power in peace and war / Michael Herman*. Cambridge, England: Cambridge University Press.

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*. Canberra: AGPS, 1984.

Johnson, L, "A Conversation with James R Clapper Jr: The Director of National Intelligence in the United States," *Intelligence and National Security Journal* 30/1 (2014), 1-25.

Jones, "Intelligence and the Management of National Security: the Post 9/11 Evolution of an Australian National Security Community,"4.

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

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*. 28 May, 2013.

Omand, D, Bartlett, J., and Miller, C. 'Introducing Social Media Intelligence

(SOCMINT)', *National Security and Intelligence Journal* 27/6 (2012), 804–6.

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, Sir Lawrence, Martin Brady, and Ken 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 National Security Issues in Policing". In *Policing in Practice,* edited by P. Birch & V. Herrington (Eds.) Sydney: Palgrave Macmillan, 2011, 109-127.

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

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 In R. Lippert, K. Walby and D. Palmer. Cham, Switzerland: Palgrave Macmillan, 2016.

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

Walsh, P.F "Building better intelligence through effective governance." *International Journal of Intelligence and CounterIntelligence,* 28(1), 2015, 123-142.

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

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