The Information Revolution and Foreign Intelligence Assessment: New Challenges for Australia?

David Schaefer

With revolutionary changes in communications technology and the growing complexity of national security, Australia's intelligence community faces a relentless growth of the information it collects and analyses. This article explores the impact of this challenge on the foreign intelligence assessment process. In particular, three risks—the threat to information security, the pressure of coordinating assessment, and the potentially harmful influence of policymakers—are examined in detail. Among other changes, a proposed Foreign Intelligence Advisory Board, modelled on the US equivalent, but with distinctive powers suited to Australia, should help minimise problems likely to arise in the years ahead.

One of the few things which can be said with any certainty about intelligence is that it is increasingly necessary for national security in the modern world. Whereas secret agencies once collected and analysed information about competitive diplomacy in the industrial age, they are now grappling with a host of novel problems, ranging from cyber espionage and weapons proliferation to health pandemics and environmental disasters.[1] Critics have argued that the complexity of this security agenda requires adjustments to the policymaking process in Australia; the task is not simply to protect against individual threats, but to chart a way through an uncertain environment with an inter-disciplinary, variegated, and systematic approach to national security.[2] As the primary means for comprehending future problems, this burden largely falls onto intelligence.

In one sense, Australia's intelligence community is well prepared for this challenge. After more than a decade of funding increases and organisational innovation, the various agencies now coordinate security operations with other parts of the government in a National Threat Assessment Centre, and are more capable of providing assistance for military operations and law enforcement. This is welcome progress, but perhaps the most vital aspect of intelligence, the capacity to inform policy, has been relatively absent in public debate or scholarly discussion about its performance in Australia. By contrast with operational concerns like

[1] William Lahneman, 'The Need for a New Intelligence Paradigm', *International Journal of Intelligence and CounterIntelligence*, vol. 23, no. 2 (2010), pp. 202-4.
[2] Alan Dupont and William Reckmeyer, 'Australia's National Security Priorities: Addressing Strategic Risk in a Globalised World', *Australian Journal of International Affairs*, vol. 66, no. 1 (2012), pp. 34-6.

catching terrorists, foreign assessment is the side of intelligence which analyses issues in defence and foreign policy for the advantage of the country's decision-makers. Despite the reformist mood of recent years, most changes seem to have barely touched on this process. In fact, the basic structure of Australia's intelligence community has remained largely undisturbed since the reforms designed by Justice Hope in the 1970s and 1980s.[3]

Within this framework, periodic efforts have been made to gauge the health of foreign intelligence assessment. Arguably the most systematic was the 2004 Flood Report, which reviewed the performance of intelligence in the lead up to the Iraq War. Flood did not point to any critical failures, but he drew attention to the declining instances of long-term assessment on foreign issues, and proposed a number of reforms to strengthen the contestability of analysis.[4] Compared with this, in 2011 the Cornall Black review, an update of Flood, reported that the intelligence community was functioning effectively, but the achievements it listed were couched in terms of security operations, with little detail offered about its contribution to the formation of policy.[5] In the absence of any proposals for reform, critics labelled the report a whitewash.[6]

Without supplying much substance, however, Cornall Black did touch on an issue which increasingly poses a challenge for the assessment side of intelligence: the growing volume of information.[7] Indeed, one implication of complexity is that, with everything connected by degrees to everything else, the breadth of detail needed to comprehend problems in national security is much wider. This has occurred alongside truly revolutionary changes in communications technology and the proliferation of electronic sources. As a result, data flows of enormous quantity are now being processed by intelligence, and these are only expected to grow as more social activity migrates onto the digital realm in the future.[8] In effect, national security is in the midst of an information revolution: with so many sources to monitor and

[3] Graeme Dobell, 'Hope's Ghost Lingers in a Secret Security World', *Inside Story*, 11 April 2012, <http://inside.org.au/hopes-ghost-lingers-in-a-secret-security-world/> [Accessed 3 October 2013].
[4] See Philip Flood, *Report of the Inquiry into Australian Intelligence Agencies* (Canberra: Commonwealth of Australia, 2004).
[5] Robert Cornall and Rufus Black, *2011 Independent Review of the Intelligence Community Report* (Canberra: Commonwealth of Australia, 2011), pp. 16-7.
[6] Paddy Gourley, 'I Spy another Intelligence Whitewash', *The Sydney Morning Herald*, 3 April 2012.
[7] Cornall and Black, *Independent Review of the Intelligence Community Report*, p. 26.
[8] William Nolte, 'Intelligence Analysis in an Uncertain Environment', in Loch Johnson (ed.), *The Oxford Handbook of National Security Intelligence* (New York: Oxford University Press, 2010), p. 415.

so many ways to do it, experts now speak about the volume of collected data as a defining challenge for the intelligence profession.[9]

The outlines of this problem were already evident at the time of the Flood Report, which proposed relocating the Open Source Centre within the intelligence community to better harness the sea of data on the internet.[10] However, this adjustment does not seem adequate when compared with the scale of the challenge; in one illustrative estimation, roughly ninety percent of the world's data is believed to have been created in the last two years alone.[11] Indeed, Allan Gyngell, a former Director-General of the Office of National Assessment (ONA), has made clear that in the intervening years, "as the volume of traditional media, new media, and social media balloons, we need to find new ways to store, search, and use it".[12] As Australia approaches ten years since Flood surveyed foreign intelligence, it is worth taking stock of this challenge: what risks does the information revolution pose for the capacity of the intelligence community to reliably inform policy?

This article investigates the issue at three separate levels of intelligence assessment: the tactical, the operational, and the strategic. In a slight divergence from the standard terminology used by intelligence scholars, the first is concerned with the issues of security for the information collected about foreign intelligence; the second deals with the production of assessment using this material; and the third focuses on the relationship between the intelligence output and policymaking. To be sure, the tactical-operational-strategic distinction is a heavily debated concept in the strategic studies literature.[13] Its use here is not intended to make any theoretical statement, but purely for reasons of analytical clarity, so that the many pressures on intelligence assessment can be distinguished.

Indeed, while most details of intelligence are guarded from public scrutiny, there are distinct trends operating at each level of assessment in Australia's intelligence community. The resulting analysis is in many ways speculative, but by examining these trends in light of the growing pressure of information, it suggests some issues will need to be addressed with more than incremental adaptation, while others are less likely to present trouble. The article concludes with an institutional reform that can strengthen what appears to be the most vulnerable area of foreign assessment for Australian intelligence in the years ahead.

---

[9] Alfred Rolington, *Strategic Intelligence for the 21st Century* (Oxford: Oxford University Press, 2013), pp. 1-4.
[10] Flood, *Report of the Inquiry into Australian Intelligence Agencies*, pp. 104-5.
[11] See for example James Risen and Eric Lichtblau, 'How the US Uses Technology to Mine More Data More Quickly', *The New York Times*, 8 June 2013.
[12] Allan Gyngell, 'The Challenges of Intelligence', Speech at the National Gallery of Australia, 30 March 2011, <http://www.lowyinstitute.org/files/pubfiles/Gyngell,_Canberra_lecture11.pdf> [Accessed 3 October 2013].
[13] For an archetypal use of the concept, see Edward Luttwak, *Strategy: The Logic of War and Peace* (Cambridge: Harvard University Press, 1987)

The Tactical Level: Information Security

Before it does anything else, intelligence must collect and distribute information. The tactical level of intelligence is concerned with the kind of material which provides assistance for active operations, such as geographic data for military planning or background detail on diplomatic negotiators. More than any other area of intelligence, this has experienced the most change in recent years.[14] The impetus behind this lies in the campaign against transnational terrorism: as foreign crises, military conflict, and home-grown radicalisation feed off one another, the many customers of intelligence need to keep up with each other so that no danger in their area goes unnoticed. As a result, the dominant trend at the tactical level of intelligence has been the growing availability of information across the many agencies involved in security operations.

Until recently, critics in Australia demanded that a similar type of overhaul be applied to the broader assessment process.[15] This has typically taken the form of complaints about intelligence being stuck in a Cold War mindset, and suggestions for a more seamless exchange of information across the community. It is part of a broader philosophy among reformist thinkers which holds that organisations relying on vertical hierarchy and centralised planning are too rigid, and should be replaced with fluid, horizontal networks to facilitate greater collaboration.[16] Indeed, many different kinds of political, social, and economic information are relevant to national security, and need to be fused together for intelligence about truly complex problems.[17] In a nod to these views, several years ago the Australian Government announced its intention to create a "smooth flow of people, ideas and activities" across the entire field of national security.[18]

But while it might be a good idea to share details about terrorism, there are risks associated with the greater availability of information throughout the intelligence workforce. In particular, digital subversion has emerged as a damaging reality. The public revelations of intelligence material by the activist group Wikileaks and Edward Snowden have seemingly exposed an

[14] Cornall and Black, *Independent Review of the Intelligence Community Report*, p. 7.
[15] See for example Carl Ungerer, *The Intelligence Reform Agenda: What Next?*, Australian Strategic Policy Institute, Policy Analysis 20, February 2008, p. 4; Sandy Gordon, 'Re-Shaping Australian Intelligence', *Security Challenges*, vol. 1, no. 1 (2005), pp. 27-58; Kevin Monks, 'Intelligence Informatics…Transforming the Australian Intelligence Community', *Journal of Policing, Intelligence, and Counter-Terrorism*, vol. 3, no. 2 (2008), pp. 62-87; and David Martin Jones, 'Intelligence and National Security: The Australian Experience', in Loch Johnson (ed.), *The Oxford Handbook of National Security Intelligence* (New York: Oxford University Press, 2010), p. 840.
[16] Andrew Rathmell, 'Towards Postmodern Intelligence', *Intelligence and National Security*, vol. 17, no. 3 (2002), pp. 98-101.
[17] William Odom, 'Intelligence Analysis', *Intelligence and National Security*, vol. 23, no. 3 (2008), pp. 323-4.
[18] Duncan Lewis, *National Security Information Environment Roadmap: 2020 Vision* (Canberra: Department of the Prime Minister and Cabinet, 2010), p. 9.

oversight in reformist thinking. In their wake, the "need to share" imperative has fallen under suspicion: among intelligence officials, there are indications of buyer's remorse, and newfound scepticism of accessible data systems.[19] In Australia, former Defence officials have echoed concerns that vitally sensitive material is being inappropriately distributed, with the clear implication that the practice should be modified.[20]

Rather than a problem for security intelligence, this may have inflicted the most damage on foreign assessment. In the case of Wikileaks, routine diplomatic reporting and military footage available to thousands of analysts were released, causing embarrassment and probably discouraging foreign sources from reaching out to US diplomats in the future.[21] Wikileaks relied on a low-level army intelligence analyst, Bradley Manning, who recorded digital copies of the classified material without arousing suspicion.[22] Similarly, Edward Snowden was able to disseminate some of the most closely guarded secrets of Five Eyes intelligence cooperation, which were nevertheless available to him on an internal intranet within the US signals intelligence agency.[23] These are concerning because unfiltered access permitted the exfiltration of as much material as was within electronic reach; once penetrated, there is seemingly little scope for limiting damage.

While internal subversion has always been a concern, the prospect of large-scale disclosures are particularly threatening in light of Australia's intelligence cooperation. After all, a wide range of information is collected by the Australian Signals Directorate (ASD), the participating agency in the 'Five Eyes' intelligence alliance between Australia, the United States, the United Kingdom, Canada, and New Zealand. Along with its partner agencies monitoring foreign communications, ASD searches electronic information across the internet and mobile telephone networks, and is privy to the resulting pool of shared material. For this reason, the agency commands uncommon respect, and media inquiries have reported "huge volumes" of "immensely valuable" information picked up through its pipeline.[24]

[19] See for example David Gioe, 'Tinker, Tailor, Leaker, Spy: The Future Costs of Mass Leaks', *The National Interest*, January-February 2014, <http://nationalinterest.org/article/tinker-tailor-leaker-spy-the-future-costs-mass-leaks-9644> [Accessed 20 January 2014].
[20] Deborah Snow, 'Spooky Silence until next Snowden Bomb', *The Sydney Morning Herald*, 23 November 2013.
[21] Bowman Miller, 'The Death of Secrecy: Need to Know…with Whom to Share', *Studies in Intelligence*, vol. 55, no. 3, 2011, <https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol.-55-no.-3/the-death-of-secrecy-need-to-know...with-whom-to-share.html> [Accessed 20 January 2014].
[22] Manning later announced his intention to undergo gender hormone therapy, and changed his name to Chelsea. To avoid any confusion, his original name and male pronouns are used here.
[23] Tom Gjelten, 'Officials: Edward Snowden's Leaks Were Masked by Job Duties', *NPR*, 18 September 2013.
[24] Philip Dorling, 'Australia Gets "Deluge" of US Secret Data, Prompting a New Data Facility', *The Age,* 13 June 2013.

The concern for Australia is that leaks via this channel unearth the sources used in foreign assessment. The little material Snowden has publicised about Australia already exposed espionage operations targeting Indonesia's political leadership.[25] With the merging of information across the intelligence community, including reports from diplomats and espionage carried out by the Australian Secret Intelligence Service (ASIS), an unprotected data store might compromise secrets across the range of intelligence activity, not simply electronic exploits by the Five Eyes. As in the Wikileaks case, foreign sources might be harmed by a systemic vulnerability in information management, or by further leaks from among intelligence partners. As the volume of data increases, in theory so does the likelihood of something being exposed.

But are leaks an inevitable by-product of information sharing in intelligence? Upon closer inspection, these examples were tailored to specific circumstances. Manning was stationed in Iraq at a tactical processing station where he could browse at will the contents of the Secure Internet Protocol Router Network, a classified intelligence network which contained material belonging to the US military and some civilian agencies like the State Department which utilised the network in order to save resources.[26] But this network existed prior to the 9/11 sharing trend; potential leakers in the US military had access to a vast trove of information for many years before he acted. What distinguished Manning was the relaxed security at his workstation: he should have been prohibited from using personal storage devices to remove data from the computer system, but this rule was not enforced at the base where he was deployed.[27] This routine security measure would have pre-empted the bulk transfer of classified information to Wikileaks, if not prohibiting his own viewing access.

The details of Snowden's activity are still uncertain, but the little that is known suggests he also exploited a specific flaw in internal security. With a background in technical support, he reportedly selected private-sector employment in Hawai'i because it offered a more relaxed security environment with intelligence access: indeed, the very software that was developed in response to Manning's leaks would have alerted Snowden's superiors to his downloading so much material off the intranet, but it had yet to be installed on the computer terminals at his location.[28] In its absence, he copied more than a million files without authorisation and escaped scrutiny because of his systems administrator privileges. There are also disputed

[25] Michael Brissenden, 'Australia Spied on Indonesia President Susilo Bambang Yudhoyono, Leaked Edward Snowden Documents Reveal', *ABC News*, 18 November 2013.
[26] Ellen Nakashima, 'Who is Wikileaks Suspect Bradley Manning?', *Washington Post*, 5 May 2011.
[27] Matt Williams and Ed Pilkington, 'Bradley Manning Hearing Told of Lax Security at Military Intelligence Unit', *The Guardian*, 19 December 2011.
[28] Mark Hosenball and Warren Strobel, 'NSA Delayed Anti-leak Software at Base where Snowden Worked—Officials', *Reuters*, 18 October 2013.

reports that he persuaded unwitting colleagues to hand over their passwords.[29]

In neither case was there a systematic vulnerability necessarily shared by Australian intelligence. Instead, relaxed information security arose from organisational strain. Manning succeeded because the US Army was fighting two wars, with morale suffering from the higher operational tempo of deployment. This was said to be the principal reason why his superiors failed to enforce the rules: they hoped that homesick, worn-out analysts would benefit from a personalised working environment, where music could be used and carried on portable discs.[30] In a similar vein, Snowden's employer, the National Security Administration, has undergone a rapid expansion in recent years: released documents speak of a "Golden Age" for signals intelligence, as the proliferation of digital information presents so many opportunities for espionage.[31] This is part of a larger trend in US intelligence which has seen the growth of private consultants, and the proliferation of security clearances for poorly monitored contractors.[32] Computer security was catching up to the risk this posed, but in Snowden's case it was not fast enough.[33]

Under pressure, the US army and intelligence community struggled to maintain best practice internal security, providing leakers with the technical opportunity to evade detection as they extracted secret documents. But while there may be occasional leaks in the future, reforms being adopted make these less likely to harm Australia. Discussions in the United States have now centred on advanced information management software which can regulate the digital activity of analysts as they search through stored data, requiring authorisation for activity like downloading.[34] This was the very protective layer which Snowden moved jobs to avoid, and Australia should make sure that a similar system is in place and regularly updated. While more emphasis on technical security cannot eliminate the threat of internal subversion, it should at least clamp down on mass-scale disclosure of secret material.

---

[29] For duelling accounts of this story, see Mark Hosenball and Warren Strobel, 'Snowden Persuaded other NSA Workers to Give Up Passwords: Source', *Reuters*, 8 November 2013; and Andy Greenberg, 'An NSA Coworker Remembers The Real Edward Snowden: A Genius Among Geniuses', *Forbes*, 16 December 2013.

[30] Nakashima, 'Who is Wikileaks Suspect Bradley Manning?'

[31] James Risen and Laura Poitras, 'NSA Report Outlined Goals for More Power', *The New York Times*, 22 November 2013.

[32] See for example Dana Priest and William Arkin, *Top Secret America: The Rise of the New American Security State* (New York: Little, Brown and Co, 2011).

[33] David Sanger and Eric Schmitt, 'Spy Chief Says Snowden Took Advantage of "Perfect Storm" of Security Lapses', *The New York Times*, 11 February 2014.

[34] Richard Clarke, Michael Morrell, Geoffrey Stone, Cass Sunstein, and Peter Swire, *Liberty and Security in a Changing World: Report and Recommendations of the President's Review Group on Intelligence and Communications Technologies* (Washington, DC: US Government, 2013), pp. 247-51.

Personnel vetting remains the best defence against subversion of this kind. Manning and Snowden both displayed behavioural characteristics which should have triggered some kind of preventative response from the organisations they were working for. Manning was reprimanded on multiple occasions for violent outbursts, but while his discharge or demotion was considered, the advice was never acted on.[35] As a privately-employed contractor, Snowden lied during his job application about past educational experience, but they hired him in spite of this because of his evident talent in computer engineering.[36] It is difficult to see an official intelligence agency committing the same error.

To avoid similar problems, Australia's foreign intelligence can best be protected from digital exposure by maintaining security standards in the face of rapid organisational change. This is a potential risk, but not as pressing as it is for US intelligence, if only because Australian national security is not nearly as expansive in scope, and less exposed to sweeping tides of growth or retrenchment. Tactical security will always present a challenge, but this should be viewed independently from the information sharing trend. Indeed, an analyst working in a walled-off, compartmentalised agency could still inflict great damage without effective monitoring. Careful attention to the institutional stability of intelligence agencies, and dedication to information security procedures, should do more to limit the risk of future leaks.

This is good news for the tactical level of intelligence, but it is only one particular issue for foreign assessment. While information sharing can be maintained, another question is whether the mass of information can be harnessed for the production of well-rounded assessment. Unlike information security, this is an area which seems more problematic.

The Operational Level: Coordinating Assessment

Between collecting information and informing policymakers, Australia's intelligence community must convert the mass of raw data into more targeted knowledge about complex issues. The production of assessment occurs at what can be described as the operational level of intelligence; as distinct from the tactical, this is an area which involves a broader range of analytical skills for interpretation, as the more enduring problems of national security are dealt with.

In recent years, a noticeable trend at this level of intelligence has been the effort to achieve a more efficient coordination of assessment resources. A dramatic statement of this intent occurred in 2008 when the Rudd Government placed the intelligence community under a National Security

[35] Richard Serrano, 'Defense Seeks Lighter Sentence for Bradley Manning in Wikileaks Case', *Los Angeles Times*, 12 August 2013.
[36] Mark Hosenball, 'NSA Contractor Hired Snowden Despite Concerns about Resume Discrepancies', *Reuters*, 20 June 2013.

Adviser (NSA) located in the Department of Prime Minister and Cabinet. Previously, ONA coordinated the various intelligence agencies, but over time this had taken a back-seat to the preparation of intelligence for the Prime Minister.[37] Instead, the NSA took over much of the responsibility for coordination with an institutionalised role: it compiles annual reports on agency performances, manages a committee to integrate intelligence functions, and promotes community-wide standards in information management.[38] As of writing, however, the fate of the NSA is uncertain: the office boasted an expansive role in the formation of national security policy, but there are reports that Prime Minister Tony Abbott has wound down this authority, if not necessarily the NSA's intelligence role.[39]

Whichever way this process goes, the trend in intelligence seems likely to reinforce more coordination from above. In part this is because of money: as Cornall Black notes, a more stringent approach to priorities could help conserve finances and eliminate unnecessary duplication across agencies.[40] The case for some kind of bureaucratic streamlining has found support from scholars concerned about the greater resources invested in intelligence over the last decade.[41] Beyond this, larger volumes of unstructured data picked up across the range of collection techniques need greater efforts to fuse them together for complex analysis. In this vein, an internal review by the Gillard Government in 2011 found serious deficiencies with the communication between agencies, criticising the patchwork of "separate ICT [Information and Communications Technology] arrangements, including data storage … with limited capacity to capture and analyse enterprise-level information". Diagnosing the problem as one of bureaucratic inertia, the report called for more integration.[42]

The assumption behind this thinking is that there is little trade-off between efficiency and comprehensiveness. Without more publicly available information this is a difficult proposition to test, but it seems insensitive to other dangers arising from the information revolution. While assessment involves the herding of various details from many sources into a coherent whole, the material needs to be scrutinised to make sure of authenticity and detail. For example, scientific expertise is needed to understand the various stages of weapons development, informants can harbour personal motivations which make them a less trustworthy source on certain issues,

[37] Peter Jennings, 'Unfinished Business: Reforming our Intelligence Agencies', *Policy*, vol. 20, no. 4 (2004-05), p. 5.
[38] Carl Ungerer, *Australia's National Security Institutions: Reform and Renewal*, Australian Strategic Policy Institute, Report 34, September 2010, p. 4.
[39] Jason Koutsoukis, 'Tony Abbott Dismantles Role of National Security Adviser by Stealth, Insiders Say', *The Sydney Morning Herald*, 25 October 2013.
[40] Cornall and Black, *Independent Review of the Intelligence Community Report*, p. 19.
[41] Peter Leahy, 'Bigger Budgets = Better Intelligence?', in Daniel Baldino (ed.), *Spooked: The Truth about Intelligence in Australia* (Sydney: NewSouth Publishing, 2013), p. 181.
[42] Philip Dorling, 'Major Flaws in Aust's Intel Sharing: Report', *The Sydney Morning Herald*, 20 July 2012.

and foreign language intercepts can have multiple meanings. Those familiar with the source of information are more likely to appreciate context, and are well positioned to tease out the potential complications.[43]

The obstacle for reform is that an arrangement which harnesses this knowledge is difficult to achieve on a more efficient basis. Multiple agencies are involved in assessment of a complex issue, but conveying the detail from analysts in one agency to another requires time and interaction, not simply greater access to one another's raw material. With the exponential growth of information, more strain is placed on these inter-agency exchanges because increasing amounts of collected intelligence will probably need to be discussed at length. Without careful attention to detail, the wrong interpretation can easily be made and disastrous consequences may result.

This was the central implication of the intelligence failure which preceded Australia's involvement in the Iraq War. By early 2003, a discrepancy had surfaced between ONA and the Defence Intelligence Organisation (DIO), the agency which focuses on strategic military affairs for the Defence Department. DIO, boasting more resources and experts with knowledge of weaponry, remained more sceptical of claims that a weapons programme existed in Iraq.[44] By contrast, ONA, tasked with a higher level of assessment to cut across many different issues, was more inclined to see a creative pattern in Saddam's behaviour. In short, the agency most familiar with the detail was better positioned to see through the ambiguity of evidence; but in the desire to integrate as much information in as little time possible, this nuance was not properly appreciated further along the process.[45]

The case of Iraq illustrates other limitations to the assessment process. The Flood Report pointed out that assumptions were often used without enough critical scrutiny.[46] In explaining his agency's record, the ONA Director-General of the time described an "accumulation of intelligence" which shaped the outlook of his analysts, whereby individual pieces of material were never verified, but presented a compelling picture when taken as a whole.[47] For example, Saddam's refusal to permit meetings between his scientists and UN inspectors was cited as likely proof that Iraq possessed prohibited weapons, but only in light of the many other instances of suspicious behaviour. With the benefit of hindsight it is known that Saddam feared international exposure of his offensive weakness would threaten his regime's stability; but at the time, what should have been interpreted as self-

[43] Calvert Jones, 'Intelligence Reform: The Logic of Information Sharing', *Intelligence and National Security*, vol. 22, no. 3 (2007), p. 390.
[44] Jennings, 'Unfinished Business', p. 8.
[45] Flood, *Report of the Inquiry into Australian Intelligence Agencies*, p. 29.
[46] Ibid., p. 25.
[47] Cited in Parliamentary Joint Committee on ASIO, ASIS and DSD, *Intelligence on Iraq's Weapons of Mass Destruction* (Canberra: Commonwealth of Australia, 2003), p. 57.

preservation was registered as another dot in a pattern of guilt.[48] As the intelligence effort against Iraq expanded, more uncertain evidence was collected to fill out the picture of a regime determined to hide something.[49]

Cognitive bias of this type will always intrude on analytical judgement. Every thinking professional has an ideological blind spot.[50] Part of this was undoubtedly due to past experience, as US intelligence had been surprised to discover Saddam's nuclear ambitions closer to realisation than had been predicted after the Gulf War. Awareness of this mistake was said to exercise great influence over analysts a decade later: while a sceptical observer might have judged the available intelligence not strong enough, a sense of urgency and the stakes involved edged assessment away from cautious detachment.[51]

But while it can never be fully avoided, there were features of the assessment process in Australia which left analysts more vulnerable to this weakness. Some knowledgeable observers of the process complained about the large volume of information received via Australia's intelligence partners, because much of this could not be properly scrutinised even as it left a strong impression in the months leading up to war.[52] An investigation by the Joint Parliamentary Committee on ASIO, ASIS and DSD did not openly endorse this view, but it did reveal that there were just three ONA staff members continually working on the Iraqi WMD angle.[53] Considering the delicacy of the subject matter, this was insufficient; and to the extent that it could have been rectified, DIO's resources had to be more thoroughly incorporated into ONA's effort.[54] In effect, coordination between the two agencies was not geared to cope with the volume of information or the complexity of the problem.

With a limited range of analytical thinking at its disposal, there appears to have been a lack of contested opinion within ONA. One publicly-known exception was Andrew Wilkie, an analyst who resigned in protest over the intelligence debate, and who took a more critical perspective than others about the agency's Iraq assessment. After scrutinising the available material, Wilkie concluded that it lacked substance and explored other motives that might have plausibly accounted for Saddam's behaviour.[55] His frustrated departure is a sign that the assessment process needs to

[48] Robert Jervis, *Why Intelligence Fails: Lessons from the Iranian Revolution and the Iraq War* (Ithaca: Cornell University Press, 2010), p. 147.
[49] Ibid., pp. 136-7.
[50] Odom, 'Intelligence Analysis', p. 327.
[51] Jervis, *Why Intelligence Fails*, pp. 138-9.
[52] Parliamentary Joint Committee, *Intelligence on Iraq's Weapons of Mass Destruction*, pp. 44-6.
[53] Ibid., pp. 46-7.
[54] Flood, *Report of the Inquiry into Australian Intelligence Agencies*, pp. 26-7.
[55] Andrew Wilkie, *Axis of Deceit: The Story of the Intelligence Officer Who Risked All to Tell the Truth about WMD and Iraq* (Melbourne: Black Inc. Agenda, 2004), pp. 81-98.

consciously maintain competitive perspectives by incorporating minority concerns, so that contrarian points are systematically addressed.

The fundamental risk at the operational level of intelligence is if a particularly compelling viewpoint or interpretation becomes ascendant, as it did in the Iraq debate. Given the growing volume of data for intelligence this could occur more frequently in the future. It is a well-established finding among intelligence experts that the reception of more information by analysts rarely dislodges settled assumptions.[56] Instead, with more material floating around than ten years ago, there is a greater chance of encountering something which validates an ingrained bias, or plays on the anxiety of the policy community. Rather than aiming to save money, coordination should be approached with an eye to resisting this pressure.

In this, diverse organisational habits and bureaucratic overlap can be a positive advantage. When efforts are made to economise on resources, the contextualised knowledge which can point out these kinds of shortcomings in assessment are at risk of being eliminated. Indeed, a misguided effort at streamlining was one of the few drawbacks to the Flood Report, which recommended that DIO's mandate be slimmed down in order to avoid wasteful duplication with ONA.[57] This undervalues the different strengths which a diverse group of analysts can offer, despite the ostensible similarity of their work. Moreover, while Flood noted the insufficient resources available for ONA at the time of the Iraq debate, this was a natural consequence of the agency's position at the apex of intelligence. Given its expansive scope, ONA is likely to struggle with the production of comprehensive assessment in time. There will probably never be the ideal level of expertise in the agency for the consideration of all the details associated with a complex issue.

Improving this situation does not call for any great change in funding. While it is unreasonable to burden ONA with the demand that every piece of data is explored with a detailed briefing from other agencies, there is also resistance to increasing manpower that would relieve ONA's workload.[58] The agency reportedly enjoys a collegiate atmosphere with a small staff and flattened hierarchy. Too much internal bureaucracy can dilute thinking, with each management layer adding more qualifications onto ideas until they lack analytical thrust in the final, consensus-driven product.[59] At its best, ONA is said to have resisted this trend, making conceptual links which push back against assumed thinking: in the case of Islamic extremism in South East Asia, it anticipated how local groups could merge into a terrorist organisation targeting Australia's diplomatic and commercial presence in the region.

[56] See Richard Heuer, *Psychology of Intelligence Analysis* (Langley: Centre for the Study of Intelligence, 1999), p. 51.
[57] Jennings, 'Unfinished Business', p. 8.
[58] Flood, *Report of the Inquiry into Australian Intelligence Agencies*, p. 109.
[59] Monks, 'Intelligence Informatics', p. 63.

Whereas their military-perspective prevented DIO analysts from noticing these signs, ONA was able to infer from socio-political trends around the world that Jemaah Islamiyah would develop into a serious threat.[60]

If not investing in more analysts, how else to cope with the abundance of information? Another proposal raised by intelligence scholars is the more rigorous use of social science methods in assessment. This would target agency practice by requiring the systematic use of techniques like the hypothetical deductive method for teasing out alternative scenarios, or the search for "negative evidence" which should have occurred if a given hypothetical were correct.[61] These are valuable analytical tools in some problem solving cases, but imposing them as a uniform standard would run the risk of weighing down the entire process with too much internal contestability. Recent research into the US intelligence community shows counter-terrorism analysts engaging in competitive one-upmanship, with a consequent narrowing of focus as new ideas about even the most marginal issues are challenged at every turn.[62] This is especially problematic because the amount of information for assessment is increasing so rapidly that it demands even more time for consultation; whereas intelligence is best served if it remains innovative.

Rather than practising blanket internal scepticism or increasing staff numbers, diverse bureaucratic input offers a better prospect for complementing assessment. This could be done by assigning staff from other agencies to issue-specific teams under guidance from ONA: an inter-agency "mosaic" of skills can be established to investigate a problem from multiple angles, without the need to ferret out every possible assumption.[63] Inter-agency teams have already been practised on issues like people smuggling, but conducted more regularly under ONA with supervision from above, they would allow that agency to direct the investigation creatively while incorporating specialised resources to bore into more detail when needed. These groups offer a way to institutionalise the dialogue which should have taken place over the Iraq assessments, with staff having to address each other's concerns in a more systematic way.

This should not be confined to government, as the private sector offers an increasingly vital source of knowledge about foreign trends relevant to national security. Intelligence officials have previously toyed with the idea of outside expertise being drafted into assessment; in this case, the temporary nature of an inter-agency group model offers a flexible way for people in

[60] Flood, *Report of the Inquiry into Australian Intelligence Agencies*, pp. 38-9.
[61] Jervis, *Why Intelligence Fails*, p. 191.
[62] Bridget Nolan, 'Information Sharing and Collaboration in the United States Intelligence Community: An Ethnographic Study of the National Counter-terrorism Center', PhD Dissertation, University of Pennsylvania, 2013, <http://media.philly.com/documents/Nolan_Dissertation.PDF> [Accessed 11 October 2013], p. 36.
[63] Rolington, *Strategic Intelligence for the 21st Century*, pp. 156-60.

business or tertiary education to be incorporated into the work of intelligence without prolonged leaves of absence.[64] The obvious drawback is the risk to information security, as more people with outside affiliations are brought into the community. But as the previous section demonstrated, the risk of an 'Australian Snowden' is a problem which should be managed with careful vetting. In fact, many of the most promising candidates are likely to be former public officials, who are more trustworthy than untested recruits. With the proximity of industry, academia, and policymaking in Canberra, the promise of stronger collaboration over intelligence problems is worthy of experimentation.

While intelligence can benefit from the inter-agency model, the challenge will be to know when it is truly needed. Sociological research suggests that a multi-party arrangement along these lines is the best way to avoid cognitive blind-spots, but that the composition of the group should not remain static.[65] Instead, periodic changes to membership would help refresh its perspective and reveal new angles worth investigating. Moreover, these teams should be viewed as a special assignment in order to receive the full cooperation of participating staff; previous attempts have been encouraging, but suffered from competition between the agencies supplying analysts, which is likely to worsen as resources are more limited than in the past.[66] For these reasons, there should be a limit to their use, and problems that might benefit from their attention will have to be prioritised. Policymakers will have to provide direction on these questions.

With the greater flow of information, coordination should be geared towards strengthening the way that multiple agencies complement one another; not simply streamlining bureaucracy. This strengthens the case for the NSA to continue supervising intelligence, and making careful use of the inter-agency model for coordinated work without marginalising nuanced thinking. The operational level of intelligence stands to benefit from these changes, but this raises issues for the next level of the intelligence process.

The Strategic Level: Policy Interface

Arguably the most difficult part of intelligence is its reception by decision-makers. This is the strategic level of intelligence; unlike the other two levels, it mixes uneasily with the role of political officials. With greater volumes of information buffeting the intelligence community, the link between assessment and the formation of policy—long a source of controversy among scholars—is being tightened, but this exposes the assessment

[64] Gyngell, 'The Challenges of Intelligence'.
[65] Susan Straus, Andrew Parker, James Bruce, and Jacob Dembosky, *The Group Matters: A Review of the Effects of Group Interaction on Processes and Outcomes in Analytic Teams*, RAND Working Paper, April 2009, <http://www.rand.org/content/dam/rand/pubs/working_papers/2009/RAND_WR580.pdf> [Accessed 20 January 2014], pp. 21-2.
[66] Ungerer, *Australia's National Security Institutions*, p. 5.

process to other risks. This section examines the resulting danger of intelligence politicisation.

It has long been recognised that the dynamics of policymaking are not sensitive to intelligence. No analyst can be expected to provide answers in a timely manner because information secured covertly is typically ambiguous; by contrast, politicians are required to take definitive action, but have limited time to acquaint themselves with the details before circumstances demand a response.[67] A clash of styles is inevitable: analysts struggle to infer connections between multiple issues while policymakers want to know why they are diverting time from their busy schedule. Operating under this constraint, intelligence is best viewed as the process of interaction between assessment and policy which narrows down the field of uncertainty for the government.[68] It requires mutual trust and continuous, frank discussion.

Since its creation as the peak intelligence agency in the 1970s, ONA has taken the lead in educating Australia's political leaders along these lines, but limited itself from doing anything that could be misconstrued as providing advice. This was to make sure that the assessment process remained free of any sense of political obligation, even as it guarantees the Director-General access to the Prime Minister. But it is rarely the case that all the implications raised by assessment are properly weighed by political leaders; they come into power with what is usually a surface understanding of the national security landscape. For this reason, ONA makes a deliberate effort to focus on issues that are relevant to the government.[69] This ensures that intelligence assessment, like military strategy, has a rational purpose by serving policy.

The trouble is that this position can subtly transform into support for the government's agenda. For instance, Wilkie argued that the proximity between ONA and senior ministers encouraged the agency to alter the emphasis of its reporting to suit the politics of selling the Iraq War.[70] The Joint Committee on ASIO, ASIS, and DSD raised concerns about the problem that the need to be "relevant" has for analytical independence, commenting on the possibility that ONA might have adjusted to the firm position of Howard ministers without being fully aware of it, if only to avoid tension.[71] Investigations by the Inspector General of Intelligence and Security (IGIS) have also focused attention on this issue: while ONA analysts do not report feeling any external pressure, the IGIS determined

[67] Arthur Hulnick, 'Intelligence Producer-Consumer Relations in the Electronic Era', *International Journal of Intelligence and Counterintelligence*, vol. 24, no. 4 (2011), pp. 748-50.
[68] Allan Behm, 'The Australian Intelligence Community in 2020', *Security Challenges*, vol. 3, no. 4 (2007), p. 5.
[69] Parliamentary Joint Committee, *Intelligence on Iraq's Weapons of Mass Destruction*, p. 54.
[70] Wilkie, *Axis of Deceit*, pp. 141-3.
[71] Parliamentary Joint Committee, *Intelligence on Iraq's Weapons of Mass Destruction*, p. 54.

several years later that it could not rule out the prospect of unconscious self-censorship taking place.[72]

This is an issue of psychology for analysts, and is correspondingly hard to diagnose. ONA's record on Iraq does not prove the existence of politicisation; after all, its mistakes were committed by intelligence services working on behalf of several governments opposed to the Iraq War.[73] But one lesson which emerges repeatedly from experience is that there is more likely to be trouble when government policy is resolute and well-advertised, as it was in the case of Iraq. For example, Des Ball illustrated how the Howard Government refused to credit the intelligence picture coming out of East Timor in its public statements during the period leading up to the outbreak of militia violence in 1999. The resistance from government officials in order to avoid diplomatic fallout may have flowed back down into the assessment process, as DIO reports temporarily became more cautious about Indonesian complicity while the evidence continued to mount.[74]

More distance between intelligence and policy can avoid this, but it is not advisable. Governments are entitled to decide which issues to prioritise, and political leaders will always draw on some mixture of personal views and past experiences.[75] As a result, if intelligence is not relevant it can end up under-utilised or bypassed. Just as pressure on intelligence analysts is harmful, so is their exclusion from the counsel of policymakers. This appears to have occurred during the 2009 Defence White Paper drafting process, when statements about Chinese military modernisation which diverged from ONA and DIO assessment were adopted. Where the intelligence agencies were more optimistic about the intent underlying Chinese behaviour, the hawkish outlook of Defence officials prevailed because they received the firm support of Prime Minister Kevin Rudd.[76] This may or may not have been the right decision, but undertaking major policy changes which resist the findings of assessment is not an encouraging sign. Indeed, a more damning indictment of the Iraq intelligence debate is that the governments involved were simply not listening; minds had been made up, irrespective of what intelligence was saying.[77]

If only to avoid becoming a wasted asset, intelligence needs to remain firmly integrated into the decision-making process. In recent years, the creation of

[72] See the Unclassified Executive Summary from Inspector General of Intelligence and Security, *Report on the Statutory Independence of the Office of National Assessments* (Canberra: Commonwealth of Australia, 2006).
[73] Paul Pillar, 'Intelligence, Policy, and the War in Iraq', *Foreign Affairs*, vol. 85, no. 2 (2006), p. 134.
[74] Desmond Ball, 'Silent Witness: Australian Intelligence and East Timor', *The Pacific Review*, vol. 14, no. 1 (2001), pp. 46-7.
[75] Odom, 'Intelligence Analysis', p. 325.
[76] Cameron Stewart and Patrick Walters, 'Spy Chiefs Cross Swords over China as Kevin Rudd Backs Defence Hawks', *The Australian*, 11 April 2009.
[77] Wilkie, *Axis of Deceit*, pp. 73-4.

the NSA was a step in this direction. A public official in the Department of Prime Minister and Cabinet, with more time than elected politicians, can offer suggestions based on a thorough understanding of intelligence. This also provides a useful locus of decision-making about inter-agency coordination. The challenge is the position's interaction with the ONA, because that agency remains the primary source of specialised knowledge for the Prime Minister. To the extent that future NSAs rely on intelligence assessment before dispensing advice, they should be in regular contact with the ONA Director-General. Indeed, that agency continues to manage subcommittees on behalf of the NSA which deal with more technical matters of resource allocation and functional integration.

However, this gives rise to a second potential for misuse. Given that it oversees intelligence, the NSA is still likely to be better acquainted with the details of assessment than any other policy figure. Armed with this knowledge, he or she might be inclined to push a particular line of interpretation at variance with intelligence findings. This appears to have been the case with the US Defense Department in the lead up to the Iraq War, where a special unit was set up to funnel information from Iraqi defectors into the assessment debate; as critics charged, this was a case of officials creating their own material to circumvent the process.[78] With the growth of information sources in the private sector, such as think tanks and risk analysis firms, there is a greater risk of rival assessment being available to policy officials.[79] Whereas the ONA Director-General previously acted as the gatekeeper of raw information, the NSA or other advisors might be tempted to operate as their own intelligence analysts.[80]

With more information at hand, intelligence may have to contend with a set of two mutually reinforcing problems. There is no escaping the fact that complex issues require more professional expertise instead of gut intuition from political officials; and this places a great premium on the relevance of intelligence assessment to policy. But with the risk that decision-makers can find information to suit their agenda when they do not receive the support they want, intelligence officials might be inclined to dip into the vast sea of unverified open source data, including social media, to supply material which retains their proximity to authority.[81] In short, the second type of politicisation identified here may heighten the likelihood of the first taking place as well.

[78] Uri Bar-Joseph and Jack Levy, 'Conscious Action and Intelligence Failure', *Political Science Quarterly*, vol. 124, no. 3 (2009), p. 475.
[79] Joshua Rovner, 'Intelligence in the Twitter Age', *International Journal of Intelligence and Counterintelligence*, vol. 26, no. 2 (2013), pp. 267-8.
[80] This is one manifestation of a more general problem mentioned in Alan Dupont, 'Intelligence for the Twenty-First Century', *Intelligence and National Security*, vol. 18, no. 4 (2003), p. 24.
[81] Rovner, 'Intelligence in the Twitter Age', pp. 267-8.

As mentioned above, while the NSA was a creation of Prime Minister Kevin Rudd, his successors attach less importance to the office. For the Abbott Government, this is reportedly motivated by a desire to re-impose Westminster tradition by shifting authority back into policy departments.[82] But there is little sign that the NSA's powers over intelligence, as opposed to policy, are curtailed. After all, before the NSA was created, ONA was required to assess its own performance; considering the vastly increased resources in recent years, this was far from ideal. Whether or not the NSA loses influence, it is unlikely to herald a shift away from closer intelligence-policy links. Even if future governments feel comfortable tackling complex problems with minimal analytical support, the delicate nature of intelligence requires closer supervision of assessment by policymakers.[83] With the revelations about the surveillance of phone numbers belonging to prominent Indonesians, more diplomatic judgement seems necessary to regulate indiscriminate espionage; if not, exposure risks imposing more costs on Australian foreign policy.[84]

Beyond that, in light of the media scrutiny and partisan debates which bedevil contemporary politics, intelligence evidence is increasingly demanded to justify government decisions, but any disclosure needs to be handled carefully so that it does not undercut policy.[85] A warning example is provided by the debate in the United States over Iranian nuclear ambitions in 2007. After a declassified National Intelligence Estimate revealed no firm evidence of a nuclear weapons programme could be found in Iran, it was seized on by opponents of the Bush administration to argue that the United States should abandon deterrence for negotiation. Lost in the media frenzy was the fact that intelligence was only referring to specific designs for building a bomb device when it mentioned "evidence"; the enrichment programme in Iran remained active, but the distinction was not emphasised in the Estimate because, in the words of one author, "we never wrote this to be read by the general public".[86] Whatever the merits of Bush administration policy, its coercive approach was undone through public misinterpretation.

Policymakers must have the capacity to shape the publication of assessment, but again, this opens up the prospect for abuse. Politicians may refer to intelligence material to confer legitimacy on their agenda, even

[82] Greg Sheridan, 'Doubling the Advisers a Sign of Global Clout', *The Australian*, 16 September 2013.
[83] For example, the same article cited above which described the Abbott Government's desire to reverse centralised policy-making at the NSA also noted that the international security advisors for the Prime Minister have doubled.
[84] See for example the blog post by former ONA Director-General Geoff Miller, 'Are We Spying Just Because We Can?', *The Interpreter*, 8 November 2013, <http://www.lowyinterpreter.org/post/2013/11/08/Are-we-spying-just-because-we-can.aspx> [Accessed 20 January 2014]
[85] Michael Wesley, 'The Politicisation of Intelligence', in Baldino (ed.), *Democratic Oversight of Intelligence Services* (Leichhardt: Federation Press, 2010), p. 198.
[86] David Sanger, *The Inheritance: The World Obama Confronts and the Challenges to American Power* (London: Bantam Press, 2009), p. 5.

if these are not truly representative of the picture conveyed by assessment. For example, during the 'Children overboard' affair statements from an ONA brief on the behaviour of asylum seekers were cited by Prime Minister John Howard, although this appears to have left the public with the wrong impression of how ONA viewed the situation.[87] The 2003 Parliamentary Inquiry into the intelligence assessment also showed this to be a problem during the Iraq debate.[88] While intelligence agencies may screen official statements to make sure that nothing is factually incorrect, they cannot disabuse the public of any mistaken impressions by issuing their own statements; in effect, this would invest them with a veto over government policy. As long as some evidence is expected by the public to justify policy choices, elected officials will have leeway to deploy intelligence for their own ends.[89] And as information increases, so does the material which can be exploited.

In sum, there are three types of misuse by the political authorities overseeing intelligence: pressuring analysts, manufacturing their own analysis, and misleading the public. With the growing volume of information, all three could occur more frequently over time. Unlike information security or inter-agency assessment, the trend towards politicisation presents a challenge which seems likely to worsen in the future unless more corrective action is taken.

A Foreign Intelligence Advisory Board

The previous three sections have outlined the major challenges which are likely to cause problems for Australia's foreign intelligence assessment. Most troublesome among these is the intelligence-policy link, which needs to be strengthened without allowing for the distortion of analytical thinking.

There are mechanisms of intelligence oversight, but nothing which is able to continuously scrutinise the assessment process with an eye to improving its policy contribution. The Parliamentary Joint Committee on Intelligence and Security reviews intelligence administration and expenditure, and at the request of a minister may investigate operational issues. But for this very reason, political interference is unlikely to be referred to the committee; only the most public controversy will see any likelihood of this happening. By contrast, the IGIS has a broad mandate to review the proprietary and legality of intelligence; in practice, this has allowed it to examine issues like the independence of assessment. But because of the many issues it needs to address across the intelligence community, it will not always be in a position to bring attention to an ongoing hole in analytical coverage, or the inadequate use of technical resources. Moreover, given the sweeping power

[87] James Cotton, *Australian Foreign Policy and the Management of Intelligence Post-September 11*, ANU Asia Pacific School of Economics and Government Discussion Paper 06-03, p. 4.
[88] Parliamentary Joint Committee, *Intelligence on Iraq's Weapons of Mass Destruction*, p. 93.
[89] Wesley, 'The Politicisation of Intelligence', p. 197.

it enjoys, the IGIS has tried to avoid seeming like a rival authority for political officials which intelligence must also answer to; if anything, it has too much authority to help without complicating things.[90]

By the same token, it is difficult to regulate the policy end of intelligence. Improved political judgement cannot be assured via bureaucratic reform: this is the task of the voting public, and politicians who emerge victorious from elections have the right to make the decisions they want. Australia's political leaders can only be implored to appoint fair-minded officials who can harness the intelligence process, whether it be the NSA or other policy advisors. While the NSA presently manages the intelligence community, it mostly draws on federal employees who are cycled through the public service without any long-term experience in the profession.[91] But more resources and expertise directly under a policy official, be it the NSA or another advisor, risks creating an opinionated staff which quarrels with ONA. The challenge is that more institutional heft is needed to aid policymakers, but without inadvertently strengthening their capacity to mishandle intelligence.

One proposal that might strike this balance is the establishment of a Foreign Intelligence Advisory Board which reports to the policymaking authority overseeing intelligence. Building on a similar model in the United States, the advisory board could be a voluntary collection of retired professionals with experience in intelligence affairs, who can regularly monitor the output of assessment and propose ideas for improving performance. As a voluntary group, the board would not require much financing, and could bring considerable expertise into an area where policymakers are typically inexperienced. Reporting independently, it could end up playing a moderating role between political advisers, who are more inclined to implement hasty reforms which serve short-term goals, and professional bureaucrats from intelligence who are more cautious about reform. Indeed, the equivalent model has at times proved vitally useful for political leaders in the United States, especially in times of rapid technological change.[92]

In order to maintain political independence, its members should be nominated by the IGIS, which has a good appreciation of the intelligence landscape; and if need be, these can be reviewed by the government, to ensure that political leaders feel comfortable with the advisors they're

[90] Ian Carnell, 'Eyes on Spies—another Platypus?', Speech at the Australian Institute of International Affairs, 22 November 2007, <http://www.aiia.asn.au/act-papers/doc_details/178-eyes-on-spies--another-platypus-ian-carnell> [Accessed 8 October 2013].
[91] Margot McCarthy, 'National Security: Past, Present, and Future', Speech at PM&C Amenities Room, 15 June 2012, <http://www.dpmc.gov.au/national_security/speeches/2012-06-15_past_present_future.pdf> [Accessed 3 October 2013].
[92] See for example the Kennedy administration's use of the board in Christopher Andrew, *For the President's Eyes Only: Secret Intelligence and the American Presidency from Washington to Bush* (New York: HarperCollins, 1995), pp. 272-3.

expected to listen to. To be sure, this also has its limitations: given that the board plays an advisory role, the lack of authority can leave it marginalised. Certainly, the US equivalent has seen its work fall on deaf ears when the policy side maintained distance from the group.[93] To avoid this problem in Australia, the board should have the power to refer problems which lie unaddressed to the Joint Parliamentary Committee: the resulting investigation may cover not only a discussion of intelligence, but also touch on the government's role in the process, as it did in the 2003 Iraq report. The board should also retain the option to publish an unclassified summary of its reporting, so that its ideas can at least have some purchase on public opinion, if not always with the government of the day. This should make it less easy to ignore those issues which the board views as most important.

With these powers in place, the advisory board would retain some capacity to ward off politicisation. Ideally, this should encourage the political leadership to extend more confidence to its members. Indeed, the board should be capable of scrutinising foreign assessment with an eye towards aiding policy, without providing a rival source of intelligence which might be expected from an empowered NSA. With greater intimacy and latitude than the IGIS enjoys, the board might also offer some advice about the political receptivity of intelligence, and ways to improve the use of intelligence in policy formation. Mistakes in the policy-intelligence relationship are more likely to be scrutinised if a larger number of experts were privy to the intelligence on which the NSA is making decisions, as at least some members from a diverse group can be expected to draw attention to the many implications for policy.

The board could also provide a useful resource for tackling the other problems canvassed in this article. The goal of streamlining the consultation between agencies would benefit from the advice of retired professionals, who know best how to capture the specific knowledge of their former employers while economising on resources. Disputes about the use of inter-agency teams for assessment could be examined in more detail and refined as the board reviews their performance. The board is also likely to offer a valuable perspective on what espionage techniques to permit, and what is not worth the risk of exposure. Given their experience, board members should also be alert to signs of organisational strain which might precede an internal security threat. Without too much power, the board has little scope for aggravating these problems; if handled correctly, however, it promises to bring more wisdom into areas which will need disciplined supervision in the years ahead.

[93] Kenneth Absher, Michael Desch, and Roman Popadiuk, *Privileged and Confidential: The Secret History of the President's Intelligence Advisory Board* (Lexington: University of Kentucky Press, 2012), p. 343.

Intelligence is too important to allow for complacency. With drastic changes in the nature and volume of information, there will have to be adjustments in the way that it is used for the purposes of national security. To address some of the likely problem areas for the intelligence community, information sharing should be preserved, despite the risk of digital subversion; a wider range of analysts from different agencies should be placed onto issue-specific groups, and private sector knowledge should be utilised. But above all, the proposal for a Foreign Intelligence Advisory Board can help strengthen what appears to be the most vulnerable part of the intelligence process in the years ahead. No change in bureaucracy is completely free of risk, but as the information revolution propels us forward, it is an institutional change from which Australia can benefit.

David Schaefer is a Non-Residential Research Fellow at the Centre for Air Power Studies in New Delhi, and an MA graduate from King's College London. *He would like to thank David Wright-Neville, Mark Schultz, and the anonymous reviewers from Security Challenges for their helpful comments on an earlier draft.* david.alexander.schaefer@gmail.com.