# SPECIAL REPORT

## Informing Australia's next independent intelligence review

### Learning from the past

Chris Taylor

June 2023

ASPI
AUSTRALIAN
STRATEGIC
POLICY
INSTITUTE

## About the author

**Chris Taylor** commenced with DFAT in 2003 and is an experienced Australian national security official currently on secondment to ASPI, where he heads the Statecraft & Intelligence program. His research includes emergent and emerging issues facing intelligence services internationally and in Australia, the place of intelligence agencies in democracies, and role of intelligence in the conduct of statecraft.

Chris' national security experience has included leadership of functions such as intelligence policy and coordination; protective security; enterprise capability; governance and oversight; and strategic futures.

In 2019-2020 Chris was a Fellow at the Harvard Kennedy School's Belfer Center for Science & International Affairs.

Chris is a graduate of the Australian National University (BA (Hons), MA (Strategic Studies)), and the University of Western Australia (Grad Dip Arts). He also holds a Diploma in Government (Security), and has completed the Harvard Kennedy School's Senior Executives in National & International Security Program and the ANU National Security College's Senior Executives Development Program.

The views expressed in this report are the author's alone and do not represent those of the Australian government or any government agency.

## Acknowledgements

The author would like to thank Stephen Merchant, Justin Bassi, Danielle Cave, Mark Watson, Dr John Coyne and Henry Campbell for their contributions to his thinking on this matter.

## About ASPI

The Australian Strategic Policy Institute was formed in 2001 as an independent, non-partisan think tank. Its core aim is to provide the Australian Government with fresh ideas on Australia's defence, security and strategic policy choices. ASPI is responsible for informing the public on a range of strategic issues, generating new thinking for government and harnessing strategic thinking internationally. ASPI's sources of funding are identified in our Annual Report, online at www.aspi.org.au and in the acknowledgements section of individual publications. ASPI remains independent in the content of the research and in all editorial judgements. It is incorporated as a company, and is governed by a Council with broad membership. ASPI's core values are collegiality, originality & innovation, quality & excellence and independence.

ASPI's publications—including this paper—are not intended in any way to express or reflect the views of the Australian Government. The opinions and recommendations in this paper are published by ASPI to promote public debate and understanding of strategic and defence issues. They reflect the personal views of the author(s) and should not be seen as representing the formal position of ASPI on any particular issue.

### Important disclaimer

This publication is designed to provide accurate and authoritative information in relation to the subject matter covered. It is provided with the understanding that the publisher is not engaged in rendering any form of professional or other advice or services.

No specific sponsorship was received
to fund production of this report.

Cover image: Magnifying glass and paper reports, iStockphoto/brazzo.

# Informing Australia's next independent intelligence review

## Learning from the past

Chris Taylor

June 2023

ASPI AUSTRALIAN STRATEGIC POLICY INSTITUTE

First published June 2023

Published in Australia by the Australian Strategic Policy Institute

ASPI
Level 2
40 Macquarie Street
Barton ACT 2600
Australia

Tel Canberra + 61 2 6270 5100
Tel Washington DC +1 202 414 7353
Email enquiries@aspi.org.au
www.aspi.org.au
www.aspistrategist.org.au

Facebook.com/ASPI.org

@ASPI_org

# Contents

# Executive summary

For a regional power such as Australia, intelligence-driven and -empowered statecraft is vital in the pursuit of some form of qualitative edge over potential adversaries (which will often have a quantitative advantage). It also happens to be an existing, if historically underappreciated, national strength for Australia—and relatively unique compared with the statecraft of many like-minded peers and other powers.

The Australian Government commissions a review of its intelligence community every five to seven years—a schedule set by the post-Iraq-War Flood review in 2004, which replaced post-mortems with proactive check-ups. July 2023 marks six years since release of the last review's report and, with funding allocated in the 2023 May federal budget, the next one is likely to commence shortly.

While there's been no major intelligence failure on which reviewers can focus, the strategic context is shifting rapidly. International power politics is back (not that it ever really went away), featuring rising global instability, Moscow's war in Europe, rising tensions in the Taiwan Strait and an increasingly aggressive Beijing. At the same time, we have had to deal with the unexpected Covid-19 pandemic, a rise in cyber intrusions and disinformation, the growing abuse of technology by authoritarian regimes, and the spectre of Australia's largest trading partner and closest ally seeking to decouple across key sectors. Important initiatives such as AUKUS, especially its second, technology, pillar, will provide new opportunities for the national intelligence community (NIC), as well as new responsibilities—not least in security and counterintelligence. Additionally, the climate crisis is increasingly seen as an issue for the intelligence community to treat as a priority rather than as a peripheral issue.

A general once-over geared to confirm a 'business-as-usual' approach will be insufficient. The upcoming review will need to grapple with some revolutionary changes already happening as well as those on the horizon, foremost among them technological game-changers such as generative artificial intelligence and an enormous growth in open-source intelligence opportunities beyond what was foreseen at the time of the last review.

Unsurprisingly, the best starting place for the review is the work that precedes it, so reflection on 2017's Independent Intelligence Review (2017 IIR) proves valuable. In this report, I make that reflection and seek to offer some lessons learned to inform the terms of reference, approach and focus of the new review.

In doing so, I identify three broad topics derived from those lessons and upon which the next review can most profitably ground its work: attracting, building and retaining a skilled workforce; adapting to rapid and profound technological change; and leveraging more, and closer, partnerships. This report highlights how the past six years have raised important and challenging questions in relation to each of those broad topics and also identifies opportunities to further advance the future performance of the NIC.

In addition, specific recommendations are made throughout the report to inform government's planning and preparation for the new review, including the following:

1. The strategic context for the next review should be aligned with the 2023 Defence Strategic Review's assessments on accelerating strategic circumstances and planning time frames.
2. The review should be tasked to produce a substantive—and substantial—public report (in addition to a classified report), including public recommendations, like the 2017 IIR:

  - but this should include a suitable level of public candour about the intelligence challenges posed to Australia by Beijing's ascendancy
  - and, post-publication, the reviewers should engage in related public dialogue and explanation, again reprising the 2017 experience.
3. At least one of the principal reviewers appointed should be female (which would be a first for an Australian intelligence review) and at least one reviewer should have detailed knowledge of, and experience within, Australian intelligence.
4. The terms of reference provided to the review should not pre-emptively constrain its consideration of future investment in NIC capability. The reviewers should be free to identify capability requirements within the bounds of fiscal realism but on the merits and without undue limitation—leaving subsequent investment decisions to government, where they most appropriately belong.
5. The review should consider whether or not the relative eclipsing of counterterrorism as an intelligence priority, and the increasing centrality of China to intelligence planning, require changes to the NIC model initiated by the 2017 IIR.
6. The review should address the 'return of the portfolio' since the NIC was established, given the resulting constraints on NIC integration. This includes consideration of how to shift from portfolio/agency-based capability development (and funding) to a more comprehensive, efficient and integrated approach—in the spirit of the 2017 IIR.
   - This includes making good on the original promises of the Joint Capability Fund and the Intelligence Capability Investment Plan.
7. The reviewers should also be tasked to undertake a follow-up public accounting of the implementation of their recommendations 18–24 months after the publication of the review's findings.

# One press conference, two announcements

On reflection, the absence of the foreign and defence ministers from the Prime Minister's press conference on 18 July 2017—especially given the actual presence of the Minister for Immigration & Border Protection and the Attorney-General, accompanied by a junior minister—was a giveaway. The government's receipt of the 'meticulous'[1] Independent Intelligence Review carried out by Michael L'Estrange AO and Stephen Merchant PSM (hereafter referred to as the 2017 IIR) would not, after all, be that evening's headline news story. However, their work would initiate the most significant structural changes to Australian intelligence since the conclusion of the first Hope royal commission, 40 years earlier.

To be fair, Prime Minister Malcolm Turnbull devoted his initial comments to acknowledging L'Estrange and Merchant's work. It was a 'landmark report', 'valuable', and with 'many important recommendations'—some of which the government had already agreed, others of which would be considered through an implementation taskforce led by the Secretary of the Department of the Prime Minister & Cabinet (PM&C).[2]

Despite the review's status as the primary announcement, the media would quickly focus attention on the parallel announcement of the creation of a Home Affairs 'super-portfolio' (see box). Modelled on the UK Home Office, this new portfolio would incorporate the erstwhile Department of Immigration & Border Protection (to be the Department of Home Affairs), the Australian Security Intelligence Organisation (ASIO), the Australian Federal Police (AFP), the Australian Transaction Reports and Analysis Centre (AUSTRAC, Australia's financial intelligence unit), the Australian Criminal Intelligence Commission (ACIC), the Australian Border Force, and the Office of Transport Security.

For the media, the Home Affairs announcement seemed inseparable from the political dynamics of the moment and a looming Liberal Party leadership challenge, which reached its denouement in the Prime Minister's eventual loss of support 13 months later.

The Home Affairs debate has rolled on ever since, with its advocates and detractors. After the 2022 election, the law enforcement agencies returned to the responsibility of the Attorney-General, but ASIO remained within the Home Affairs portfolio, and the portfolio itself was confirmed as a bipartisan feature of Australia's national-security architecture.

Lost in the public discourse was the importance of the 2017 IIR itself.

## The seeds for Home Affairs planted in 2015

The most substantive official consideration of the Home Affairs proposal prior to July 2017 can be found in January 2015's Review of Australia's Counter Terrorism Machinery, as carried out by PM&C. That report canvassed the potential benefits arising from a 'small, coordinating Department of Home Affairs based loosely on the UK Home Office', finding that '[t]his Review agrees with the conclusion reached by the Smith Review[3] that a small, coordinating Department of Home Affairs could be effective at leading Australia's [counterterrorism] effort if the department focussed on strategic issues,' and that such a department could 'oversight all relevant domestic intelligence and law enforcement agencies'.[4]

In addition, PM&C's review acknowledged the view (ironically, given subsequent criticism[5] of the removal of certain national-security functions from the Attorney-General's responsibilities) that:

> Currently, the Attorney-General must balance his duties as first law officer of the Commonwealth with his national security responsibilities, including bringing forward measures restricting or even removing the rights of certain individuals.
>
> Appointing a separate minister responsible for a Department of Homeland Security could free the Attorney-General to take a more unimpeded view of the legal ramifications and consequences of national security proposals.[6]

However, the review, highlighting practical difficulties both in the operation of a Home Affairs portfolio and the separation of the extant legal and national-security functions of the Attorney-General, concluded that:

> In respect of [counterterrorism], this Review therefore concludes there is no compelling reason to change the current system of ministerial oversight and departmental structures. Rather, it should be retained and strengthened.[7]

# Background: what was the 2017 IIR tasked to do and what did it find?

Distinguished and experienced national-security officials,[8] L'Estrange and Merchant were commissioned by Prime Minister Turnbull to conduct the second review of the intelligence community since Philip Flood's review in 2004.[9] Commencing in November 2016, they were to prepare findings and recommendations on the Australian intelligence community (AIC),[10] including:

> … the relationship and engagement between [AIC] agencies and the members of the broader National Intelligence Community, including the Australian Federal Police, the Department of Immigration and Border Protection, the Australian Criminal Intelligence Commission, and the Australian Transaction Reports and Analysis Centre.
>
> The review [would] consider, among other things:
>
> - how the key aspects of our security environment and the nature of security threats have changed in recent times, including as a result of technological advancements, and how they are likely to change further over the coming ten years or so
> - how effectively the AIC serves (and is positioned to serve) Australian national interests and the needs of Australian policy makers
> - whether the AIC is structured appropriately, including in ensuring effective co-ordination and contestability
> - whether the AIC is resourced appropriately, including to ensure the right balance of resources across the AIC and that agency resources are properly matched against national security priorities, and the impact of the efficiency dividend
> - whether legislative changes are needed, including to the *Intelligence Services Act 2001*
> - whether capability gaps, including technological, are emerging and how these might be met, noting potential efficiencies and that any new proposals would need to be consistent with the Government's overall fiscal strategy
> - the effectiveness of current oversight and evaluation arrangements
> - the development path of overseas intelligence partners and lessons for Australia.[11]

After months of study, interviews and submissions, the 2017 IIR identified the principal challenges and drivers affecting the AIC as:

- developments in new forms of inter-state rivalry
- extremism (especially Islamist terrorism)
- accelerating technological change
- new frontiers of data-rich intelligence and related risks to the existing intelligence model.[12]

The 2017 review acknowledged significant growth and maturity in the AIC since 2011. The AIC's annual budget was approaching A$2 billion, and it now had almost 7,000 staff.[13] Furthermore, the AIC was performing well. However, there was the opportunity to take individual (agency) excellence to an 'even higher level of collective performance' through strengthened integration.[14] The objective was the attainment of a ‘world class intelligence community’—requiring changes to intelligence-community management and coordinating structures, new funding mechanisms, streamlining of some legislative arrangements, and measures to further strengthen trust between agencies and the Australian community.[15]

As a result, the 2017 IIR made 23 recommendations.[16] Some of the most impactful recommendations that resulted in major change for Australian intelligence included:

- the establishment of an Office of National Intelligence (ONI) out of an expanded and empowered Office of National Assessments (ONA), with the Director-General of ONI serving as ‘head of the National Intelligence Community (NIC)’ and principal intelligence adviser to the Prime Minister
- the establishment of a Joint Capability Fund (JCF) and Intelligence Capability Investment Plan (ICIP) to underpin future capability development
- the statutory independence of the Australian Signals Directorate (ASD) from the Department of Defence
- a future, comprehensive, review of national-security legislation
- expanded remits for the Inspector-General of Intelligence & Security (IGIS) and for the Parliamentary Joint Committee on Intelligence & Security (PJCIS).

More implicitly, and importantly, the 2017 IIR reconfigured Australian intelligence around the 10-agency-strong NIC, and away from the ‘traditional’ six-agency AIC—with the promise of a truly *national* intelligence enterprise incorporating mutually empowering security, foreign, law-enforcement and border intelligences.

# The 2017 IIR's notable insights

The review's unclassified report, published in June 2017, offered three notable insights into the challenges and opportunities facing Australian intelligence: profound changes in the international system—with consequences for intelligence; an increasingly challenging operational environment; and a pressing need for integration and greater interagency coordination and cooperation.

Unsurprisingly, given its authorship, the 2017 IIR was characterised by a sophistication concerning 'fundamental *changes in the international system*'[17] and their consequences for intelligence—similar to that displayed by Flood. For instance:

> In this environment, power politics remains important in the rivalry and competition among states, and there are signs that it will become more accentuated over coming years. Espionage and counter-espionage have always been realities in the power politics of the modern international system. That remains the case and it will intensify and evolve in unpredictable ways.[18]
>
> … Australia's ability to protect and advance its security interests will depend critically on how well it understands the complex forces of change that are evolving. It will also depend on how effectively it addresses the challenges and utilises the opportunities they present. Australia's intelligence agencies have a vitally important role to play in achieving these outcomes.[19]

Furthermore, the 2017 IIR quoted British diplomat Sir Roderic Braithwaite's observation that '[s]ecret intelligence is needed to combat secretive adversaries.'[20]

As with Flood, the 2017 IIR also spoke candidly of the limits to intelligence:

> Secret intelligence has no special status simply because it is acquired by secret means. Moreover, because it often deals with reasonable probabilities and not absolute certainties, intelligence rarely provides clear-cut guarantees about the future. Nor is it appropriate for intelligence agencies to recommend policy directions to government.[21]

And, insightfully:

> [S]ome of the issues that intelligence agencies address are 'puzzles' (to which answers exist), others are 'mysteries' (on which, at best, insights are more relevant than answers). Mostly, the role of intelligence is not to predict the future but to explain the forces at work in particular situations and thus to help government influence developments.[22]

The 2017 IIR noted heightened expectations of government and the public when it came to intelligence, including those flowing from the expectations of expatriates and travellers about the Australian Government's obligations to them when they're overseas.[23] It also reflected on how the previously stark division between intelligence collectors and assessors was now less clear. Collectors, for example, now had a need for analysis to directly support operations, while their assessment colleagues needed their own means of open-source intelligence (OSINT) collection.[24]

The review also identified some fundamental emerging challenges for the conduct of intelligence activities, including undertaking human-intelligence (HUMINT) operations in overseas environments, owing to:

> … advances in surveillance technology and its increasingly widespread use in urban environments [which] increase the difficulty of conducting clandestine human intelligence operations overseas. This will be compounded by enhanced capabilities for establishing the true identity of individuals with a high degree of reliability. These realities create an increasingly formidable operational environment for intelligence agencies.[25]

This has since been accentuated and accelerated by the impact of Covid-19 and an authoritarian turn in many countries.[26]

Notably, the 2017 IIR zeroed in on the opportunities that *integration and more collective approaches* to capability presented to Australian intelligence. This included skewering the 'familiar contention' that the relative smallness of the AIC (at least compared to the US and UK intelligence communities), and close interactions between its members meant that informal linkages could substitute for more concrete, structured coordination.[27]

This would find expression in recommendations for the JCF and ICIP. Those new capability investment measures would become the first substantive capability collaboration and community-based funding initiatives within the NIC:

- *Joint Capability Fund*: a 'fund to support technological innovation and the development of shared capabilities designed to be used across the different agencies'.[28] This would be administered by ONI, would include competing bids, and could be drawn upon for capability development benefiting more than a single agency.
- *Intelligence Capability Investment Plan*: a consolidated plan capturing major investments proposed by NIC agencies over the forward estimates that would provide suitable context for 'government to make better informed decisions on the inevitable capability trade-offs that will be needed in future years, and to provide agencies with a greater degree of certainty about their future budgetary outlook to assist forward planning'.[29] The ICIP would be furnished annually to ministers by ONI, alongside an accounting of existing NIC funding.

And, of course, there was the promise of the NIC itself—bringing together all the elements of national intelligence (security, foreign, law enforcement and border protection) into a single enterprise and underpinned by structural initiatives such as the evolution of ONA into ONI and the statutory independence of ASD.

# Positive approach taken by the reviewers

Beyond its content, there was much merit in the general approach taken by L'Estrange and Merchant, who were aided by the great confidence held in them by stakeholders. Their public report, extending to 130 substantive pages, was a worthy successor to Flood's similarly substantive approach to publication in 2004 and set the intelligence community on solid ground until the next scheduled review. This was further demonstrated by the openness of the reviewers to post-report commentary and explanation, including in contextualising the parallel Home Affairs initiative.[30]

This was a very different approach from that which had been adopted by the 2011 Independent Review of the Intelligence Community (see box). In addition, the 2017 public report sparked a variety of academic and policy analysis, contributing to the further development of an intelligence dialogue in Australia.[31]

## The Cornall–Black review of 2011

Between Flood's seminal 2004 review and 2017 came a review commissioned by the Gillard government and completed in 2011, undertaken by former Secretary of the Attorney-General's Department Robert Cornall AO and ethicist and McKinsey consultant Rufus Black (now Vice Chancellor of the University of Tasmania). The Cornall–Black review's reception was dented by their much more limited approach to the unclassified version of their report than had been taken in 2004 or would be taken in 2017. Unfortunately, the publicly released version contained no recommendations and ran to only 57 pages (much of which was appendixes, bland descriptions of the make-up of the AIC or definitions of basic intelligence terminology).[32]

Another factor in this impression of constraint was the fiscal environment and directly imposed lack of ambition, captured in the subtitle from Chapter 3 ('Meeting the new security challenges in a time of constrained resources') and explicit in the terms of reference ('noting that any future proposals would need to be offset consistent with the Government's overall fiscal strategy').[33] A better approach would have been to free the review to identify—on the merits—what capability recommendations were needed and then consider capability options arising from those recommendations in the normal course of expenditure review. This isn't to say that the intelligence budget should be unbounded (it shouldn't), but the responsibility shouldn't be on the intelligence community and reviewers to ignore realities. Instead, responsibility to make the tough fiscal decisions should fall to the political class. A common past criticism was that agencies and the broader bureaucracy too often prejudged National Security Committee of Cabinet (NSC) decision-making and, as a result, were reluctant to bring related requirements to the NSC.

The Cornall–Black report was supportive of outcomes delivered by the AIC between 2004 and 2011, giving examples including counterterrorism, support to military operations, the disruption of people smuggling, counterproliferation, counterespionage and cybersecurity. The reviewers also lauded the AIC's international relationships.[34]

*The opportunities for reform* identified in the public report were improved priority setting, mission integration and intelligence distribution; more efficient and rigorous performance evaluation; external input to support innovation; new strategies for managing intelligence collection in an age of abundant information; continuing to enhance working relationships within the AIC; and continuing to deepen the quality of working relationships with the broader national-security community.[35]

# An accelerating future and the perils of implementation (and politics)

It would be unrealistic to expect that a report as comprehensive as the 2017 IIR could predict the future with unerring accuracy, that its conclusions would be unimpeachable, or that the implementation of its recommendations would be total.

While, as I've noted, the review captured emerging trends in Australia's strategic environment, it was reticent about acknowledging, at least in the public version, China's central part in those developments—and indeed China's centrality to Australia's national-security thinking. The public report mentions China just twice—both times paired with India in vanilla references to global power shifts.[36] Nor does the report identify the phenomena of the 'grey zone' or information operations (and misinformation and disinformation), although it does deal with the emergent challenge of foreign interference (about which a classified review had been undertaken simultaneously, leading to new foreign interference laws).

Just three years later, the 2020 Defence Strategic Update would publicly identify that '[s]trategic competition, primarily between the United States and China, will be the principal driver of strategic dynamics in our region' and that 'major powers have become more assertive in advancing their strategic preferences and seeking to exert influence, including China's active pursuit of greater influence in the Indo-Pacific'.[37] The Defence Strategic Update would also highlight the 'grey zone' as a phenomenon that, while not new, was one for which 'Defence must be better prepared … including by working more closely with other elements of Australia's national power.'[38] Interestingly, 2023's unclassified version of the Defence Strategic Review would complete the circle by omitting reference to the 'grey zone'.[39]

That acknowledgment of China's centrality to Australian security considerations jars with the 2017 reviewers' assessment that:

> For Australia's intelligence agencies, in particular, the forces of strategic change are *broadening* their responsibilities, *diversifying* their operational priorities and creating new requirements for a more integrated focus.[40] [emphases added]

In the context of 2023, it's at least arguable that, rather than broadening and diversifying, developments in Australia's strategic circumstances are having the effect of *clarifying* and *focusing* priorities around China as disruptive strategic actor, counterintelligence threat and capability pacesetter. China's aggressive rise presents multiple challenges to Australian policymaking, including in spaces once considered chiefly 'domestic', such as national resilience and social cohesion, economic policy, critical infrastructure, and responses to misinformation and disinformation. With such a wide range of threats and vulnerabilities, the extended NIC (that is, including Home Affairs, ACIC, the AFP and AUSTRAC) brings relevant capability advantages.[41]

It's for the upcoming independent review to judge whether the clarification and focus brought to Australian intelligence thinking by an ascendant China requires the NIC model established by the 2017 IIR to be updated or modified.

There's also a question of whether the 2017 IIR overestimated the extent to which counterterrorism would remain among the NIC's foremost priorities. That was entirely understandable just three years after the declaration of the caliphate of Islamic State in Iraq and Syria (ISIS), and following numerous ISIS-inspired terrorist outrages (including in Australia) both leading into and during the review period—and before the anti-ISIS victories in the months following the report's release.[42] Although the 2017 IIR's specific judgements about global extremism (especially the impact of online extremism) remain salient, the report did miss the degree to which counterterrorism would be eclipsed by a refocusing on the more traditional concern of strategic competition and state-on-state rivalry and conflict.[43]

In addition, the 2017 IIR, while making some recommendations in relation to the *Intelligence Services Act 2001* (principally concerning ministerial authorisations[44]), kicked the can of legislative reform down the road to a future, more comprehensive, review of national-security legislation—the result being the voluminous but unsatisfying (and for the public, unclear and unconcise) four-volume report produced by Dennis Richardson AC and released publicly in December 2020.[45]

Other developments were beyond the responsibility of the reviewers. As I've noted, parallel initiation of a Home Affairs portfolio—a development that was outside of the IIR's remit—had a significant impact. Less distortionary but still consequential was the subsequent development of a more joined-up (even with ASD's independence) organisation of Defence intelligence under the new three-star Chief of Defence Intelligence, bringing a greater degree of integration to the management of Defence's civilian, joint and single-service intelligence capabilities.

The most significant effect of those developments was a 'return of the portfolio', in the words of ASPI's 2021 'Collaborative and Agile' research project, with a resulting check on NIC integration.[46] Prior to the changes made last year, of the 10 NIC agencies, five were in the Home Affairs portfolio and three were in the Defence portfolio (both portfolios with their own vast budget hinterlands and staffing), with the Australian Secret Intelligence Service (ASIS) and ONI standing alone in the Foreign Affairs and Prime Minister's portfolios, respectively. While this wasn't a significant mathematical change from the pre-2017 portfolio arrangements (that is, with the Attorney-General's portfolio standing in for Home Affairs), the inclusion of the Department of Home Affairs as a NIC member itself and its explicit national-security mission (distinct from the Attorney-General's Department) meant that the Home Affairs portfolio developed a distinct identity inside the NIC, including prioritisation of portfolio-based planning and budgeting. What was true for Home Affairs was also true for the Defence portfolio. This didn't halt NIC-level integration, but slowed and distorted it.

The other factor outside of the reviewers' control was implementation. The Australian Government has to date not provided a comprehensive accounting of the implementation (or otherwise) of the 2017 IIR's 23 recommendations.[47] As I've noted, when releasing the report, Prime Minister Turnbull indicated that there were recommendations that the government immediately accepted (not all were specified, but the architectural and statutory changes to ONI and ASD were), and the remainder were to be addressed through a departmental process.[48] While there will always be elements of the implementation that will need to remain classified, the failure to provide this accounting has done the public a disservice, including by limiting the ability of external analysts to hold government and agencies accountable for delivery.

However, the two most significant institutional and structural changes to the intelligence community were indeed made and are apparent today. First, ONI came into being in 2018, replacing ONA, with the passage of the *Office of National Intelligence Act 2018* and the appointment of Nick Warner AO PSM as the first Director-General of ONI. Second, ASD became a statutory agency, within the Defence portfolio but, importantly, especially for its national cybersecurity responsibilities, outside the Defence Department. Ministers, agencies and individuals refer by default to the NIC, and the 10 agencies all feature in the institutional functioning of the NIC and publicity concerning the community. So, too, with the majority of integrative recommendations dependent on the ONI and NIC changes, such as the exercise of ONI's coordination function (known within the community as 'enterprise management'), its leadership structure, and so on.

As I've noted, the Richardson review was subsequently undertaken, and its findings on the NIC's legal framework were made public. Also, most (but not all) of the changes to ministerial authorisations per recommendations 16 and 18 were implemented. The government did not support recommendation 19 regarding certain weapons authorisations to be devolved to the ASIS Director-General.

Importantly, the government did support recommendation 22 for the enhanced resourcing of the IGIS. Although both the current and former IGISs have since publicly acknowledged practical challenges to recruiting staff to meet that enhanced resourcing (and responsibilities)—most notably (but in common with the rest of government), lengthy delays in obtaining security clearances.[49]

Of note, the 2017 IIR's recommendations (21 and 23) in relation to the PJCIS and IGIS, including the extension of IGIS and PJCIS remits to the four non-AIC agencies in the NIC and a step towards parliamentary oversight of operational matters,[50] haven't yet been implemented in full.[51] In November 2022, the Attorney-General told the Australian Parliament that changes in relation to the IGIS and PJCIS were still being contemplated.[52] On 22 June 2023 he introduced into the parliament the Intelligence Services Legislation Amendment Bill. Broader questions of the appropriate remit, responsibilities and make-up of the PJCIS remain very much alive.[53]

It's apparent that other recommendations, even where agreed, have been only partially implemented. The JCF and ICIP were introduced and remain as mechanisms within the NIC, but their form and resourcing proved considerably more limited than was envisaged by the review. So, for example, the recommendation that the JCF be funded from, and to the extent of, the efficiency dividend drawn from NIC agencies (or parts thereof, in the case of those departments or agencies in which intelligence was only a component) wasn't taken up by government. It also appears that the government didn't take up the review's suggestion that the inaugural ICIP include defined options (that is, real growth of 1.5% and 3% from 2018–19) for longer term growth in NIC resourcing.

The consequences of those decisions by government have been to limit the levers available to the Director-General of ONI to incentivise collaborative approaches to capability development—and to alternatively disincentivise more traditional portfolio-based capability bids. Those implementation issues exacerbated the Director-General's existing constraints resulting from the 2017 IIR's conclusion that ONI shouldn't exercise direct control over agency budgets.[54] This budget issue has also been a major one for our closest allies, the US and UK, which deal with the matter differently (the US has individual agency budgets, whereas there's a hybrid in the UK with a 'single intelligence account' from which the Secret Intelligence Service (MI6), MI5 and Government Communications Headquarters are funded and which is managed collaboratively between the agencies). This budgetary challenge should be a key question examined in the upcoming review.

Recommendation 12 in the review regarding top-secret positive vetting gave the beleaguered Australian Government Security Vetting Agency an initial reprieve in relation to the highest level (positive vetting, PV) security clearances. As foreshadowed by the 2017 IIR, that reprieve has now been superseded by the transfer of all PV clearances from that agency and other authorised agencies to a new authority within ASIO, following passage of the ASIO Amendment Bill on 22 June 2023.[55]

# Time for the next independent intelligence review

One of the most valuable outcomes of Philip Flood's 2004 review was securing successive governments' commitment to regular, proactive reviews of the intelligence community—a move from post-mortems to check-ups. As noted above, this July marks the sixth anniversary of the L'Estrange–Merchant review's release. In short, it is now, literally, time for a new intelligence review.

Furthermore, it's critical that Australia's national intelligence capabilities are evaluated in the whole and against our accelerating strategic circumstances, including the 2023 Defence Strategic Review's conclusion that: 'Instead of a 10-year warning time, the Review has identified three distinct time periods for Defence planning: the three-year period 2023–2025 (for those matters which must be prioritised and addressed urgently); the five-year period 2026–2030; and the period 2031 and beyond.'[56]

Of course, history has shown that many consequential changes are made after a crisis (for example, the Flood review following the Iraq fiasco and legislative changes following ISIS's rise). There's a dual risk: relying on post-mortem reviews can result in lurches made through urgency, not necessity (as happened after 9/11). And a check-up review not born from a specific event or crisis can be undertaken with a sense of routine that confirms the *status quo* (for example, the Cornall–Black review). The latter seems to be a particular risk today and should be avoided by the yet to be announced review team.

The 2017 review is an example of a review that wasn't established due to a specific event but was still empowered to examine what changes were needed to stay ahead of threats. The same went for the 2016–17 review into foreign interference. This upcoming review should be similarly empowered as the 2016–17 reviews and undertaken in a similar context to the 2023 Defence Strategic Review; that is, not because of a single event affecting Australia, but as a proactive review in the context of a strategic environment that's far worse than it was only six years ago due to war in Europe, pandemics, climate change, Beijing's aggressive rise and the use of technology in ways once almost unimaginable. Now is the time for such a proactive review, not a routine check-up that merely seeks to confirm a business-as-usual approach. The world is changing and, even where structural change isn't recommended, cultural, legal, resourcing and capability enhancements are all vital for the terms of reference.

For a regional power such as Australia, intelligence-driven and -empowered statecraft is vital in the pursuit of some form of qualitative edge over potential adversaries (which will often have a quantitative advantage). It also happens to be an existing, if historically underappreciated, national strength for Australia—and relatively unique compared with the statecraft of many like-minded peers (and even more significant powers, such as Japan).

Historically, regional intelligence sectors have been focused on internal security, reflecting postcolonial priorities in state formation and development. Separately, in Japan's case, intelligence-sector development was, until the 21st century, fragmented and underprioritised (reflecting its own historical legacies) and remains nascent, although the past year has seen significant defence reforms that will probably begin to flow into intelligence.[57] Australia was the only one of the 'other three eyes' (Australia, New Zealand, Canada) to establish a foreign HUMINT service (and did so in 1952).[58] Similarly unique is Australia's creation of a specific agency to undertake geospatial intelligence functions (note that it remains within the Defence Department).[59]

Intelligence can also be a valuable sovereign capability. Yes, there are aspects of Australia's intelligence cooperation model similar to (and some more intimate than) the allied interoperability of Defence.[60] But there are other aspects that are much more definitively (and defiantly) sovereign—and (per Flood), rigorous, open-eyed and independently informed intelligence assessment is the key to making sovereign decisions in our strategic circumstances. So, too, is the wielding of intelligence diplomacy as a national capability—bolstered by the reputation of Australian intelligence internationally.[61]

# Lessons from 2017 for a future review

In addition to several one-off matters that would be pertinent for a future review to consider (for example, the enduring impact of the pandemic on intelligence operations and capabilities, notwithstanding that this subject has had some past examination by the PJCIS), there are three broad matters from which a lead can be taken from the 2017 IIR: workforce, technology, and the power of partnerships.

## Attracting, building and retaining a skilled workforce

First, the existential challenge for NIC agencies is in finding, attracting and retaining the skilled workforce capable of tackling technological and operational challenges—and also meeting the significant growth and transformation needs of those agencies. This needs to be a central focus for a future review. As just one example, ASD's decade-long REDSPICE transformation alone requires the recruitment of 1,900 new (and net) staff.[62] If anything, the sceptical observations of the 2017 IIR about the capacity of the NIC to meet workforce requirements understated the degree to which workforce issues challenge the NIC's future effectiveness. This planned workforce expansion is happening amid relatively low unemployment, the resulting very competitive market for talented and highly skilled workers, compounded by lengthy and discouraging recruitment processes (especially as a result of security-clearance delays) and a disconnect between workplace opportunities inside and outside the NIC (for example, the limited availability of work-from-home options, access to personal devices, and so on, with their disproportionate impact on younger prospective employees).

Linked inextricably with this requirement to significantly grow the intelligence workforce is the need to broaden the aperture of entry to that workforce and make a career in intelligence a practical and attractive option for a much broader—and considerably more diverse—range of Australians. This has significant implications for security-clearance and recruitment practices, for how the NIC communicates with the public, and what it's willing to share about the community's work—as well as a willingness to be open to genuinely incorporating cultural diversity into how the NIC goes about that work.

This challenge isn't unique to intelligence agencies, as similar circumstances are facing the ADF,[63] but the ADF's requirements only serve to exacerbate the NIC's predicament. It will be vital for the forthcoming review to identify and examine alternative options to the *status quo* when it comes to future workforce needs—including more centralised and directive NIC-based approaches.[64]

Attention should also be paid to the development and enablement of staff once they're inside the NIC. This includes the conscious incentivisation, and potential mandating, of cross-agency career pathways for intelligence leaders. While the strong organisational cultures of the individual NIC agencies are a strength, organisational culture that depends on inculcating and perpetuating narrow views is unwelcome and corrosive.[65]

## Adapting to rapid technological change

Second, technology looms as another important challenge for the future NIC, more particularly the adoption and effective utilisation in an intelligence context of emergent and emerging technologies, including artificial intelligence / machine learning (AI/ML), biotechnologies and augmentation, and quantum computing (with its threat and promise in relation to encryption). This includes the suitable integration of technology needs and initiatives between the NIC and Pillar 2 of the AUKUS agreement.

The technological challenge is perhaps most acute when it comes to the opportunities presented by the superabundance of open-source data and the integration of such data with secrets—to ultimate intelligence effect. This isn't a new challenge, as much of the past 20 years has been spent by agencies on the development of such techniques, but getting it right remains an aspiration. AI/ML looms as a solution but one that raises significant issues, especially if automating decision-making.[66]

The key is that OSINT and secret intelligence work hand in hand. The fact that there's now more openly available data than ever shouldn't be viewed as a substitute for, or replacement of, secret intelligence. If anything, the abundance adds an extra burden to intelligence agencies and requires more resourcing and effort to actually make use of OSINT, including to separate fact from fiction or to decipher a combination of the two ('faction') while continuing to collect and analyse the harder to find classified and secret intelligence that we need to do three things: first, confirm what's in open source; second, identify open-source disinformation; and, finally, reveal what simply isn't in the public domain.[67]

## Leveraging more and closer partnerships

Third is the need for more, and even closer, partnerships. Workforce and technology challenges demand more effective approaches to capability development within the NIC but also in partnership with the broader national-security community (including Defence), with industry and civil society, which are often at the forefront of technology and open source, and with international counterparts. As I've noted, the 2017 IIR took substantive steps in this direction, notably through the creation of the JCF and the ICIP. However, the partial implementation of the review's recommendations (including suboptimal resourcing) has led back to a much more portfolio-siloed approach to capability development.

The positive take is that there's still much that could be achieved through greater jointery—including more ambitious approaches to shared services and foundational capabilities across multiple agencies, if not across the entirety of the NIC.

Relatedly, there's a vexed question of how best to govern, resource and evaluate the broader national-security community (including the other tools of statecraft, such as diplomacy, development aid and the military). It makes little sense to focus only on how capability development occurs within the NIC, given the significant crossover of needs and effects with Defence, the Department of Foreign Affairs & Trade and other agencies. The 2017 IIR's terms of reference denied the reviewers the opportunity to explore this aspect of national decision-making, including the ideal of a comprehensive national-security budget. The result is an understandable frustration on the part of ministers in successive governments about such processes.

As to the structure and make-up of the NIC, a future review will need to consider whether our deteriorated strategic circumstances since 2017 require additional institutional arrangements. An example would be whether existing arrangements provide suitable net assessments of China's military and other national capabilities, especially those most likely to be used in any future coercion of Australia and its lines of trade and international communication—and thereby derive and track effective warning indicators. A joint-agency centre, drawn from the NIC and Defence planners, might effectively enhance related individual agency-level capabilities, such as within the Defence Intelligence Organisation.[68]

Given the impact for the 2017 IIR occasioned by the Home Affairs initiative, it would therefore be prudent for future reviewers to bear in mind today's analogue—a potential return of the National Security Adviser concept—when drawing their conclusions about the NIC's future. The National Security Adviser concept,[69] still alive today, would be unlikely to be part of an intelligence review's terms of reference but it would be directly relevant to the review's considerations and findings, especially as to NIC structure. A government even semi-seriously considering such an option for the future should ensure that its intelligence reviewers are formally included in its confidences.[70]

Another issue that's arisen in the context of previous reviews but for which a satisfying answer remains elusive is how policymakers (ministers and officials) can more effectively utilise intelligence. This includes the problem of intelligence consumption and a perceived oversupply of (sometimes scattergun) intelligence reporting. Reviews have naturally focused on the intelligence community end of the equation (after all, that's the remit of intelligence reviews), but there are opportunities for improvement at the customer end. Few reviews have, to date, engaged substantively with the evolving information-consumption habits and preferences of emerging leaders.

Then there are the related issues of public profile and the social licence for intelligence within the Australian community. These continue to be underdeveloped, despite the recent efforts of individual agency heads, and will be critical to successfully resolving the capability challenges for the NIC described herein.

## Approach and reviewers

There are also lessons to be drawn from the 2017 IIR as to the approach to be taken by a future review—and by the government when commissioning such a review. I've noted above, for example, the importance of releasing a substantive and substantial public version of the review's findings (per 2004 and 2017, and *vice* 2011). A future review should build on that approach and buttress its recommendations for further reforms with as open and clear a case to the public as possible.

Importantly, none of the previous reviews of Australian intelligence has been conducted by a woman, and it would be beneficial and important for at least one of the future reviewers to be female.[71] Comparison of past reviews also suggests that the quality of review findings is significantly enhanced by at least one of the reviewers having a deep, working knowledge of intelligence matters.[72] (Justice Hope was the outlier in this regard, but of a different era.)

# Appendix: Recommendations of the 2017 IIR

## Structure/architecture

***Recommendation 1***: An Office of National Intelligence (ONI) be established as a statutory authority within the Prime Minister's portfolio, and that:

a) ONI be led by a Director-General (DG ONI) and this appointment be at departmental Secretary level;

b) DG ONI be the head of the National Intelligence Community (NIC) as well as the Prime Minister's principal adviser on intelligence community issues, with the role including advice on the appointment of senior NIC office-holders and succession planning;

c) DG ONI be a member of the Secretaries Committee on National Security;

d) without directing the specific activities of agencies, DG ONI be able to direct the co-ordination of the NIC to ensure there are appropriately integrated strategies across the suite of NIC capabilities;

e) DG ONI chair an expanded National Intelligence Co-ordination Committee and that its membership include the Chief of the Defence Force or their representative;

f) DG ONI chair a new Intelligence Integration Board;

g) DG ONI's roles and responsibilities be supported by a new legislative mandate which would include the provision of statutory independence for the position of DG ONI; and

h) DG ONI be accountable to the Prime Minister and the National Security Committee of Cabinet for the performance of the NIC generally, and agencies in particular, in relation to National Intelligence Priorities and the provision of relevant input to Ministerial and Cabinet decision-making. (report paragraphs 4.18 to 4.28)

***Recommendation 2***: The Office of National Intelligence (ONI) encompass two main areas of responsibility led by Deputy Directors-General (at the Senior Executive Service Band 3 level) responsible for Intelligence Enterprise Management (including intelligence integration) and Assessments, and that:

a) the Director-General ONI (DG ONI) be given the authority and responsibility for advising government on intelligence collection and assessment priorities, and allocating responsibility for intelligence collection across the intelligence agencies;

b) DG ONI report to the Prime Minister and the National Security Committee of Cabinet on a regular basis to provide a holistic view of performance against priorities and to make recommendations on ways of closing intelligence gaps, making choices among relative priorities, and in consultation with the heads of relevant intelligence and policy agencies ensuring the appropriate mix of coverage;

c) DG ONI have responsibility for new arrangements for agency evaluation that are appropriately rigorous across specific mandates, that are similar to the Functional and Efficiency Reviews currently led by the Department of Finance, that are conducted by senior ONI and Department of Finance staff supplemented as appropriate by competent experienced external reviewers, and that make practical assessments of progress in relation to prioritisation, effectiveness, resource allocation, capability development and co-ordination; and

d) DG ONI provide the Prime Minister with a written personal overview every two weeks on key issues for the intelligence agencies, and that this overview be supplemented by meetings with the Prime Minister every two weeks. (paragraphs 4.29 to 4.38)

***Recommendation 3:*** Integration in areas of high intelligence focus be improved by:

a) establishing a dedicated Office of National Intelligence (ONI) position to facilitate closer co-ordination, evaluation and integration across national counter-terrorism intelligence activities as a whole;

b) the Australian Cyber Security Centre (ACSC) operating as part of the Australian Signals Directorate (ASD), and that:

i) staff from other agencies be seconded to the ACSC but also retain their existing organisational authorities and ability to access data, information and capabilities from their home organisations;

ii) a Head of the ACSC be appointed as the single focus of accountability to the Government for cyber security, and provide a six-monthly report to Cabinet on proposed cyber security priorities, progress in implementing them and emerging cyber issues;

iii) one Minister have primary responsibility for the ACSC and cyber security under arrangements to be determined by the Prime Minister, noting that the authorities under which ASD would continue to operate would derive from the Minister for Defence (as currently required by section 3A of the *Intelligence Services Act 2001*);

iv) an Intelligence Co-ordinator for Cyber Security be appointed to more effectively meet and manage the growing expectations of the ACSC, particularly in safeguarding the security of government networks, responding to incidents, and providing the intelligence to support policy and international engagement;

v) governance of the ACSC be provided by the current Cyber Security Board chaired by the Secretary of the Department of the Prime Minister and Cabinet, and in addition to its existing membership the Board also include Director-General ONI and CEO-level representatives of critical national infrastructure sectors including telecommunications, health care, financial institutions, other services, energy, water and ports;

vi) ASD's legislative mandate specify its role as the national information and cyber security authority, including functions to combat cyber crime and to provide advice to the private sector on cyber security matters; and

vii) ACSC's cyber hotline for Government agencies and the private sector operate 24 hours a day, 7 days a week, and a 24/7 capability to manage public messaging and policy advice in relation to rapidly emerging cyber events also be established. (paragraphs 4.39 to 4.56)

***Recommendation 4***: The Office of National Intelligence (ONI) be responsible for leading and co-ordinating data management and ICT connectivity initiatives across the National Intelligence Community, and that the Open Source Centre be integrated into ONI's Intelligence Enterprise Management role and enhanced as a centre of expertise for open source collection, analysis, tradecraft and training. (paragraphs 4.57 to 4.61)

***Recommendation 5***: Current Office of National Assessments analyst numbers be increased by at least 50 per cent to support the Office of National Intelligence's (ONI) intelligence assessment role, and that:

a) ONI be responsible for preparing a morning Daily Brief for the Prime Minister on intelligence issues of significance;

b) an ONI Assessment Consultation Board be established, chaired by the Director-General ONI and consisting of senior leaders from ONI, other intelligence agencies and relevant policy departments as well as individuals from business, non-government organisations, universities and think-tanks who can add relevant perspectives to intelligence assessment matters; and

c) ONI develop a more intensive and substantive program of interaction with experts outside of government to inform assessments. (paragraphs 4.62 to 4.69)

***Recommendation 6***: The Australian Signals Directorate (ASD) be made a statutory authority within the Defence portfolio reporting directly to the Minister for Defence, and that:

a) the Head of ASD be appointed at a level of seniority equivalent to the Directors-General of the Australian Security Intelligence Organisation and the Australian Secret Intelligence Service;

b) the existing organisational arrangements that integrate the support to military operations capability within ASD be reaffirmed and strengthened;

c) a senior military officer be appointed as the principal ASD Deputy Director at a rank commensurate with the responsibilities and accountabilities of the role; and

d) a dedicated joint ASD–Defence team be established to manage ASD's transition to a statutory authority, drawing on relevant expertise within and outside of government, and reporting to the National Security Committee of Cabinet. (paragraphs 4.70 to 4.80)

## Capability/funding

***Recommendation 7***: A Joint Capability Fund administered by the Office of National Intelligence be established to support the development of shared capabilities, with the total amount in the Fund being equivalent to the Efficiency Dividend levied on the intelligence agencies. (paragraphs 5.29 to 5.42)

***Recommendation 8***: Changes be made to the application of the Efficiency Dividend to the intelligence agencies as follows:

a) the Efficiency Dividend be applied to 100 per cent of Australian Signals Directorate (ASD) funding with effect two years after ASD's establishment as a statutory authority; and

b) the Efficiency Dividend be applied to 100 per cent of the funding of the Office of National Intelligence (ONI) with effect two years after ONI's establishment as a statutory authority. (paragraphs 5.38 to 5.39)

***Recommendation 9***: An Intelligence Capability Investment Plan (ICIP) be established that identifies the major capability projects that agencies seek agreement to commence over the period of the Forward Estimates, and that the Director-General of the Office of National Intelligence prepare the ICIP annually for consideration by the National Security Committee of Cabinet, noting that:

a) The ICIP should also be presented in conjunction with a comprehensive overview of the National Intelligence Community's (NIC) existing funding and commitments.

b) The ICIP should include the projects which the Australian Signals Directorate (ASD) has in Defence's Integrated Investment Program (DIIP), and that the associated funding be transferred from the Defence budget to ASD after it transitions to a statutory authority. The current phases of ASD's DIIP funding should continue to be administered by the Department of Defence, and over time, later phases of existing projects, as well as their replacements and future projects, should move into the ICIP.

c) The ICIP, in its first iteration, be presented to government with options for overall funding envelopes based on NIC funding and indexed at 1.5 and 3 per cent real growth per year, with effect from 2018–19. (paragraphs 5.43 to 5.54)

***Recommendation 10***: Proposals for new funding for important long-term intelligence capability initiatives be assessed against agreed principles, including: a) additional funding should be focused primarily on Australia's own intelligence needs; b) the likely return on investment should be specified; and c) funding should be phased over time and subject to periodic review against objectives. (paragraphs 5.26 to 5.27)

***Recommendation 11***: The Office of National Intelligence be responsible for developing and overseeing the implementation of a strategic approach to the development of the National Intelligence Community workforce as part of its intelligence enterprise management responsibilities. (paragraphs 5.5 to 5.12)

***Recommendation 12***: The Australian Security Intelligence Organisation receive additional resourcing to allow it to second staff to the Australian Government Security Vetting Agency (AGSVA) as soon as possible, and that the situation with AGSVA Top Secret (Positive Vetting) clearances be reviewed in early 2018 to allow time for the current remediation program to have effect. If processing times still exceed six months, alternative options for Top Secret (Positive Vetting) clearances should be explored. (paragraphs 5.13 to 5.14)

***Recommendation 13***: Data analytics and ICT connectivity, including the establishment of an intelligence community computing environment in which technical barriers to collaboration are minimised, be one of the highest priorities of a more structured approach to technological change and for the funding of joint capabilities. (paragraphs 5.15 to 5.19)

***Recommendation 14***: The Office of National Intelligence lead a more structured approach to the National Intelligence Community's responses to technological change, with a high priority given to:

a) establishing a National Intelligence Community Science and Technology Advisory Board;

b) creating a National Intelligence Community Innovation Fund to support the development of prototypes for transitioning research outcomes into operational systems; and

c) supporting a National Intelligence Community Innovation Hub to facilitate ways in which government, industry and academia could come together to address capability needs and solutions and create new linkages. (paragraphs 5.20 to 5.25)

## Legislation

***Recommendation 15***: A comprehensive review of the Acts governing Australia's intelligence community be undertaken to ensure agencies operate under a legislative framework which is clear, coherent and contains consistent protections for Australians. This review should be carried out by an eminent and suitably qualified individual or number of individuals, supported by a small team of security and intelligence law experts with operational knowledge of the workings of the intelligence community. (paragraphs 6.7 to 6.19)

***Recommendation 16***: Amendments to the Ministerial authorisation (MA) regime in the *Intelligence Services Act 2001* (ISA) and associated processes be made to address practical difficulties arising from implementation of the regime. Such amendments, to be pursued in advance of the comprehensive review recommended above, would include:

a) Introducing a class-based MA regime to enable ISA agencies to produce intelligence on a class of Australian persons involved with proscribed terrorist organisations. The class authorisation should be issued by the responsible Minister with the agreement of the Attorney-General and overseen by the Inspector-General of Intelligence and Security (IGIS). Class authorisations should last for a maximum period of six months but could be renewed. ISA agencies should maintain a current list of the Australians on whom they are seeking to produce intelligence on under the authorisation, outlining the justification for their continued coverage. Agencies should have to report to the responsible Minister within six months of the original authorisation.

b) Introducing a class-based MA regime to enable ISA agencies to undertake activities to produce intelligence on Australian persons when the agencies are operating in support of the Australian Defence Force (ADF). This regime would be subject to the same oversight requirements as recommended above in relation to class authorisations for Australian persons involved with proscribed terrorist organisations.

c) Introducing a requirement for all ISA agencies to seek an MA for activities likely to have a direct effect on an Australian person.

d) Requiring ISA agencies to obtain MAs only for activities involving the use of covert collection capabilities by including a definition of 'producing intelligence' in the ISA. For the Australian Secret Intelligence Service, Ministerial authorisation should continue to be required for tasking an agent or network of agents to produce intelligence on an Australian person or class of Australian person overseas, or when requesting an international partner to do likewise. We also recommend amending the definition of 'intelligence information' in the ISA.

e) Permitting an ISA agency to act immediately and without an MA in situations where it is reasonable to believe that an Australian person consents to the ISA agency producing intelligence on that person. In these circumstances, the ISA agency should be required to notify the responsible Minister and the IGIS as soon as possible and at a maximum, within 48 hours. In situations involving a threat to security, the Minister responsible for the Australian Security Intelligence Organisation (ASIO) should also be advised.

f) Providing that when an MA involves a threat to security, the Minister responsible for the ISA agency first consider the case prepared by their own agency in consultation with ASIO. If the Minister agrees with the arguments presented by the ISA agency, the Minister should then consult with and obtain the agreement of the Attorney-General before issuing the authorisation. (paragraphs 6.30 to 6.51)

***Recommendation 17***: Regular briefings be held involving the 'Agency Heads' (as defined by the *Intelligence Services Act 2001*), their responsible Ministers, and the Attorney-General and Director-General of Security, on intelligence collection activities overseas which, if compromised, could impact on Australia's foreign policy or international relations. (paragraphs 6.52 to 6.53)

***Recommendation 18***: The co-operation provisions in Divisions 2 and 3 of Part 3 of the *Intelligence Services Act 2001* (ISA) be streamlined to enhance co-operation amongst agencies. These changes, also to be pursued in advance of the comprehensive review recommended above, would include:

a) clarifying that two ISA agencies co-operating with one another can act jointly under a single Ministerial authorisation from the relevant Ministers; and

b) extending the co-operation regime for activities undertaken in relation to the Australian Security Intelligence Organisation to all ISA agencies and to activities undertaken both within and outside Australia. (paragraphs 6.54 to 6.62)

***Recommendation 19***: The Director-General of the Australian Secret Intelligence Service (ASIS) be able to authorise activities under Schedule 2 of the *Intelligence Services Act 2001* concerning the use of weapons and self-defence techniques by ASIS staff members and persons co-operating with ASIS. In addition to the existing requirement in relation to notifying the Inspector-General of Intelligence and Security, the Director-General should also be required to notify the Minister responsible for ASIS of any new authorisations or changes to existing authorisations on a monthly basis. (paragraphs 6.63 to 6.67)

***Recommendation 20***: Existing consultation arrangements for the development of legislative reform proposals be strengthened to ensure legislative amendments are coherent and progressed in a timely manner. (paragraphs 6.68 to 6.74)

## Oversight

***Recommendation 21***: 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, with oversight of the Australian Federal Police, the Department of Immigration and Border Protection, and the Australian Criminal Intelligence Commission limited to their intelligence functions, and with current oversight arrangements in relation to the Office of National Assessments applied to the Office of National Intelligence. (paragraphs 7.19 to 7.22)

***Recommendation 22***: The Office of the Inspector-General of Intelligence and Security be allocated additional resources to enable it to sustain a full-time staff of around 50. (paragraphs 7.23 to 7.27)

***Recommendation 23***: The role of the Parliamentary Joint Committee on Intelligence and Security (PJCIS) be expanded by amending relevant legislation to include:

a) a provision enabling the PJCIS to request the Inspector-General of Intelligence and Security (IGIS) conduct an inquiry into the legality and propriety of particular operational activities of the National Intelligence Community (NIC) agencies, and to provide a report to the PJCIS, Prime Minister and the responsible Minister;

b) a provision enabling the PJCIS to review proposed reforms to counter-terrorism and national security legislation, and to review all such expiring legislation;

c) provisions allowing the PJCIS to initiate its own inquiries into the administration and expenditure of the ten intelligence agencies of the NIC as well as proposed or existing provisions in counter-terrorism and national security law, and to review all such expiring legislation;

d) provisions enabling the PJCIS to request a briefing from the Independent National Security Legislation Monitor (the Monitor), to ask the Monitor to provide the PJCIS with a report on matters referred by the PJCIS, and for the Monitor to provide the PJCIS with the outcome of the Monitor's inquiries into existing legislation at the same time as the Monitor provides such reports to the responsible Minister; and

e) a requirement for the PJCIS to be regularly briefed by the Director-General of the Office of National Intelligence, and separately by the IGIS. (paragraphs 7.28 to 7.47)

# Notes

[1] Graeme Dobell, 'The making of the Australian intelligence community', *The Strategist*, 15 June 2020, online.

[2] Malcolm Turnbull, 'National security announcement', transcript, 18 July 2017, online.

[3] This is a reference to the 2008 Review of Homeland & Border Security carried out by Mr Ric Smith AO PSM. Summary and conclusions as in *Summary and conclusions: Report of the Review of Homeland and Border Security*, 4 December 2008, online.

[4] Department of the Prime Minister & Cabinet (PM&C), *Review of Australia's Counter Terrorism Machinery,* Australian Government, 2015, 23–24, online.

[5] For example, see comments from the then shadow Attorney-General: 'Home Affairs too much power for one: Labor', *SBS News*, 8 May 2018, online. In addition, see the Australian Federal Police Association's comments in Christopher Knaus, 'Federal police must split from Dutton ministry to save integrity, says union', *The Guardian*, 15 March 2019, online, and subsequently in Anna Macdonald, 'AFP switches back to A-G department, ASIO stays in Home Affairs', *The Mandarin*, 2 June 2022, online. See also, Michael Pelly, '"Back where it belongs": police association praises portfolio shift', *Australian Financial Review*, 2 June 2022, online; John Blaxland, 'New home affairs department seems to be more about politics than reform', Strategic & Defence Studies Centre, Australian National University, 20 July 2017, online.

[6] PM&C, *Review of Australia's Counter Terrorism Machinery*, 23.

[7] PM&C, *Review of Australia's Counter Terrorism Machinery*, 26.

[8] L'Estrange had served as Cabinet Secretary, High Commissioner in London, Secretary of the Department of Foreign Affairs & Trade and head of the National Security College at the Australian National University. Merchant had been Deputy Secretary of the Department of Defence and a doyen of the intelligence community—including as Director of the (then) Defence Signals Directorate. L'Estrange and Merchant were assisted, as an adviser, by Sir Iain Lobban KCMG CB, former director of the UK's General Communications Headquarters (GCHQ). With his expertise and background with DSD, Merchant's selection was directly linked to the strong emphasis in the review's terms of reference on the implications of technology for future intelligence.

[9] The first review post-Flood was carried out by former Secretary of the Attorney-General's Department Robert Cornall AO and management consultant / ethicist Rufus Black in 2011. See later box.

[10] That is (in 2016), ASIO, the Australian Secret Intelligence Service (ASIS), the Australian Signals Directorate (ASD), the Defence Intelligence Organisation (DIO), the Australian Geospatial-Intelligence Organisation and the Office of National Assessments (ONA).

[11] PM&C, *2017 Independent Intelligence Review*, Australian Government, June 2017, 11–12, online.

[12] PM&C, *2017 Independent Intelligence Review*, 5–6.

[13] PM&C, *2017 Independent Intelligence Review*, 7.

[14] PM&C, *2017 Independent Intelligence Review*, 5.

[15] PM&C, *2017 Independent Intelligence Review*, 5.

[16] PM&C, *2017 Independent Intelligence Review*, 13–22. The full list of recommendations is included in the Appendix of this paper.

[17] PM&C, *2017 Independent Intelligence Review*, 23.

[18] PM&C, *2017 Independent Intelligence Review*, 24.

[19] PM&C, *2017 Independent Intelligence Review*, 25. See also 31–32.

[20] PM&C, *2017 Independent Intelligence Review*, 32, citing 'Defending British spies: the uses and abuses of intelligence', address to the Royal Institute of International Affairs, Chatham House, 5 December 2003.

[21] PM&C, *2017 Independent Intelligence Review*, 32. Although, we would go further and note that intelligence, whether through insight or effect, can't fix broken—or indeed absent—policy. For example, the 2017 IIR invoked the continuing importance of economic intelligence (p. 49), echoing Justice Hope. But, in the absence of strategic economic policy, is economic intelligence a viable activity?

[22] PM&C, *2017 Independent Intelligence Review*, 33. In reference to 'mysteries' and 'puzzles', the review cited Gregory F Treverton's *Reshaping national intelligence for an Age of Information*, Cambridge University Press, 2001, 11–13.

[23] PM&C, *2017 Independent Intelligence Review*, 25.

[24] PM&C, *2017 Independent Intelligence Review*, 37.

[25] PM&C, *2017 Independent Intelligence Review*, 39.

[26] See Danielle Cave, 'Data driven: How COVID-19 and cyberspace are changing spycraft', *Australian Foreign Affairs*, 9, July 2020, 29–52, online. See also then ASIS Director-General Paul Symon, 'Foreign espionage: an Australian perspective', address to the Lowy Institute, 10 May 2022, online.

27 PM&C, *2017 Independent Intelligence Review*, 55.

28 PM&C, *2017 Independent Intelligence Review*, 7.

29 PM&C, *2017 Independent Intelligence Review*, 8.

30 See, for example, Michael L'Estrange's five-part interview series with Graeme Dobell, ASPI, *YouTube*, August 2017, online.

31 For example, in the subsequent work of ASPI, the Australian National University's National Security College and Strategic & Defence Studies Centre, the Lowy Institute, the United States Studies Centre, etc.

32 PM&C, *2011 Independent Review of the Intelligence Community report*, Australian Government, November 2011, online.

33 The explicit reference to offsets marks this out as distinct from the terms of reference for the 2017 IIR (previously cited) and meant that any new intelligence spending/capability would need to be directly offset—implicitly from existing intelligence activities or capabilities.

34 PM&C, *2011 Independent Review of the Intelligence Community report*, 16–17.

35 PM&C, *2011 Independent Review of the Intelligence Community report*, 17–22.

36 PM&C, *2017 Independent Intelligence Review*, 23, 24.

37 Department of Defence (DoD), *2020 Defence Strategic Update*, Australian Government, 2020, 11, online.

38 DoD, *2020 Defence Strategic Update*, 5.

39 The closest the DSR would come to this concept publicly would be its discussion of coercion short of invasion; see *National Defence: Defence Strategic Review*, Australian Government, 2023, 25, online.

40 PM&C, *2017 Independent Intelligence Review*, 28–29.

41 In 2021, ASPI proposed an alternative organising principle for the NIC, oriented around the 'China Mission'. More than just an intelligence priority, it was envisaged as the basis for organisational transformation and a lens through which to see the intelligence task (aligned to other strategic initiatives). See Michael Shoebridge, John Coyne, Rajiv Shah, *Collaborative and agile: intelligence community collaboration insights from the United Kingdom and the United States*, ASPI, Canberra, 2021, online.

42 For useful background, see the timeline prepared by the Wilson Center, 'Rise, spread and fall of the Islamic State', 28 October 2019, online.

43 Notably, the 2017 US National Security Strategy's primary focus was on the new era of strategic competition.

44 See Chapter 6 of PM&C, *2017 Independent Intelligence Review*.

45 Attorney-General's Department, *Report of the Comprehensive Review of the Legal Framework of the National Intelligence Community*, Australian Government, 4 December 2020, online.

46 See Michael Shoebridge, John Coyne, Rajiv Shah, 'Strengthening intelligence collaboration in Australia: lessons from the UK and the US', *The Strategist*, 25 November 2021, online.

47 A full list of the 2017 IIR's recommendations is in the Appendix to this paper.

48 The change in Prime Minister (from Turnbull to Scott Morrison) would necessarily disrupt implementation and indeed the precise role of Director-General of National Intelligence (given Turnbull's part in the position's design).

49 See, for example, Sarah Basford Canales, 'Security vetting queue for public servants a "black box": IGIS Christopher Jessup', *Canberra Times*, 28 October 2022 (updated 30 October 2022), online, and the late Hon Margaret Stone AO's last appearance before the Parliamentary Joint Committee on Intelligence & Security, 7 August 2020, online. See also Kate Grayson, 'Intelligence watchdog faces continuing staffing deficit', *The Strategist*, 9 March 2022, online.

50 Via a PJCIS request to IGIS to conduct an inquiry and report back to the committee.

51 While the Richardson review endorsed the mechanism for IGIS to conduct inquiries at the request of the PJCIS, it opposed the extension of IGIS's remit to the non-AIC agencies. See Attorney-General's Department, *Report of the Comprehensive Review of the Legal Framework of the National Intelligence Community*, Australian Government, 4 December 2020, 1(55), online.

52 During introduction in the House of Representatives of the separate—now passed—IGIS (Modernisation) Bill 2022.

53 See, for example, Kate Grayson, 'Gatekeeping the parliamentary intelligence committee won't make Australia safer', *The Strategist*, 19 May 2023, online. As an aside: it would be prudent for opponents of an expanded remit for the PJCIS (that is, into operations) to consider whether operational equities will be better safeguarded by the kind of compromise measures recommended by the 2017 IIR or take a chance on the findings of a future review (or indeed an initiative from the parliament itself).

54 PM&C, *2017 Independent Intelligence Review*, 58

55 Legislation before the Senate at the time of writing. See also Home Affairs Minister Clare O'Neil, 'Enhanced security and vetting clearance capabilities for ASIO', 29 March 2023, online. For further background on this initiative, see Chris Taylor, 'Classifications and clearances are the bricks and mortar of national security', *The Strategist*, 20 June 2023, online.

56 *National Defence: Defence Strategic Review*, Australian Government, 2023, online.

57 The best single-volume, English-language history of Japanese intelligence remains Richard J Samuels, *Special duty: a history of the Japanese intelligence community*, Cornell University Press, 2019.

58 With the establishment of the Australian Secret Intelligence Service, although ASIS wasn't publicly acknowledged until 1977.

59 The Australian Geospatial-Intelligence Agency. The Canadian and New Zealand equivalents (the Canadian Forces Joint Imagery Centre and GEOINT New Zealand, respectively) are better characterised as elements of those nations' broader military-intelligence capabilities.

60 See, for example, short statement on ADF, ASD and US Cyber Command pursuit of '… collective advantage in cyberspace through integration across the areas of defensive cyber operations, capability development, training and exercises', from AUS-US Cyber Dialogue 2022, online.

61 Australia's use of intelligence diplomacy is the subject of a separate forthcoming report from ASPI's Statecraft & Intelligence Program.

62 Australian Signals Directorate, *REDSPICE: A blueprint for growing ASD's capabilities*, Australian Government, 2022, online.

63 Richard Marles, ‘Address to the Sydney Institute Annual Dinner Lecture, 14 November 2022’, online.

64 By way of example, see the whole of US intelligence community recruitment campaign coordinated by the Office of the Director of National Intelligence, online.

65 A point made well in relation to the broader Australian policy community in Asia–Pacific Development, Diplomacy & Defence Dialogue’s options paper, *What does it look like for Australia to … use all tools of statecraft in practice*, 2023, 15, 28, online.

66 An alternative approach to the technology future for the NIC (and the particular challenge of leveraging data) is given by Dr Miah Hammond-Errey in *Secrecy, sovereignty & sharing: how data and emerging technologies are transforming intelligence*, United States Studies Centre, February 2023, online.

67 Further consideration of the relationship between OSINT and secret intelligence can be found in Justin Bassi, Chris Taylor, ‘Australia’s intelligence community must adapt to stay ahead of the game’, *The Strategist*, 22 May 2023 (first published in the *Canberra Times* on 20 May 2023), online.

68 We are indebted to Stephen Merchant for this example and suggestion.

69 Between 2008 and 2013, a National Security Adviser position existed within PM&C (at its most senior at an Associate Secretary level) to coordinate national-security policymaking and advise the Prime Minister and the Secretary of PM&C. The inaugural National Security Adviser, a departmental official rather than a political or statutory appointee, was Major General Duncan Lewis AO DSC CSC (later Director-General of ASIO).

70 Such a government should also consider why the initial national security adviser concept wasn’t a success and was ultimately ceased. This includes the importance of ensuring that the position is grounded on more than just individual abilities and is given suitable levers in relation to national security (whether that’s through legislation, budget arrangements, resources or some other means). It would also be well advised to resist the lure of too expansive an ‘all hazards’ approach to national security, on whose rocks the previous initiative ran aground.

71 Alex Oliver, Danielle Cave, ‘Australia’s intelligence community needs another independent review’, *The Interpreter*, Lowy Institute, 9 March 2020, online.

72 Notably former ONA Director-General Philip Flood (2004) and former DSD Director Stephen Merchant (2017).

# Acronyms and abbreviations

| | |
|---|---|
| 2017 IIR | 2017 Independent Intelligence Review |
| ACIC | Australian Criminal Intelligence Commission |
| ADF | Australian Defence Force |
| AFP | Australian Federal Police |
| AI/ML | artificial intelligence / machine learning |
| AIC | Australian intelligence community |
| ASD | Australian Signals Directorate |
| ASIO | Australian Security Intelligence Organisation |
| ASIS | Australian Secret Intelligence Service |
| AUSTRAC | Australian Transaction Reports and Analysis Centre |
| DG ONI | Director-General, ONI |
| HUMINT | human intelligence |
| ICIP | Intelligence Capability Investment Plan |
| ISA | *Intelligence Services Act 2001* |
| ISIS | Islamic State in Iraq and Syria |
| JCF | Joint Capability Fund |
| MA | ministerial authorisation |
| NIC | national intelligence community |
| NSC | National Security Committee of Cabinet |
| ONA | Office of National Assessments |
| ONI | Office of National Intelligence |
| OSINT | open-source intelligence |
| PJCIS | Parliamentary Joint Committee on Intelligence & Security |
| PM&C | Department of the Prime Minister and Cabinet |
| PV | positive vetting |

## Some recent ASPI publications

STRATEGY

'Impactful projection'

Long-range strike options for Australia

Marcus Hellyer and Andrew Nicholls

December 2022

ASPI AUSTRALIAN STRATEGIC POLICY INSTITUTE

SPECIAL REPORT

'Impactful mateship'

Strengthening the US–Australia defence relationship through enhanced mutual understanding

Colonel Alan W Throop

May 2023

ASPI AUSTRALIAN STRATEGIC POLICY INSTITUTE

NORTHERN AUSTRALIA STRATEGIC POLICY CENTRE

SPECIAL REPORT

Deciding the future

The Australian Army and the infantry fighting vehicle

Dr Albert Palazzo

October 2022

ASPI AUSTRALIAN STRATEGIC POLICY INSTITUTE

SPECIAL REPORT

The geopolitical implications of Russia's invasion of Ukraine

Paul Dibb

September 2022

ASPI AUSTRALIAN STRATEGIC POLICY INSTITUTE

SPECIAL REPORT

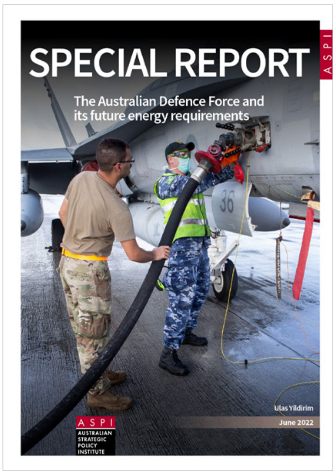
Smooth sailing?

How Australia, New Zealand and the United States partner in—and with—the Pacific islands

Joanne Wallis and Anna Powles

May 2023

ASPI AUSTRALIAN STRATEGIC POLICY INSTITUTE


SPECIAL REPORT

The Australian Defence Force and its future energy requirements

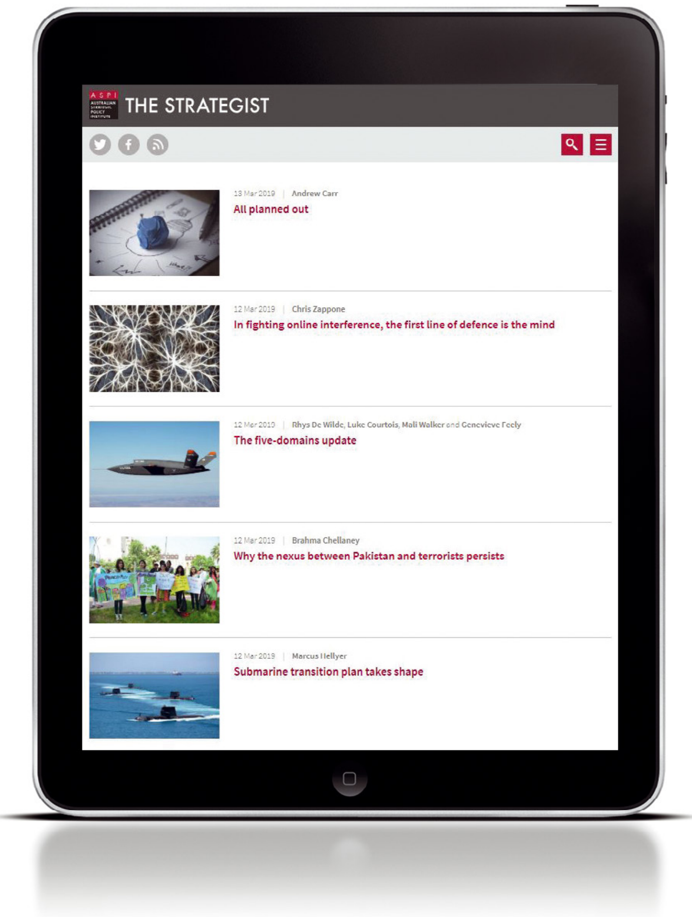
Ulas Yildirim

June 2022

ASPI AUSTRALIAN STRATEGIC POLICY INSTITUTE

## Stay informed via the field's leading think tank, the Australian Strategic Policy Institute.

***The Strategist***, ASPI's commentary and analysis website, delivers fresh ideas on Australia's defence and strategic policy choices as well as encouraging discussion and debate among interested stakeholders in the online strategy community. Visit and subscribe to an email digest at www.aspistrategist.org.au.


THE STRATEGIST

13 Mar 2019 | Andrew Carr
All planned out

12 Mar 2019 | Chris Zappone
In fighting online interference, the first line of defence is the mind

12 Mar 2019 | Rhys De Wilde, Luke Courtois, Mali Walker and Genevieve Feely
The five-domains update

12 Mar 2019 | Brahma Chellaney
Why the nexus between Pakistan and terrorists persists

12 Mar 2019 | Marcus Hellyer
Submarine transition plan takes shape

facebook.com/ASPI.org

@ASPI_org

A S P I
AUSTRALIAN
STRATEGIC
POLICY
INSTITUTE

To find out more about ASPI go to www.aspi.org.au
or contact us on 02 6270 5100 and enquiries@aspi.org.au.

# Informing Australia's next independent intelligence review

Learning from the past

ISSN 2200-6648