Match-fit for the global contest?

Innovation, leadership, culture and the future of Australia's National Intelligence Community

CHRIS TAYLOR

ASPI
AUSTRALIAN STRATEGIC POLICY INSTITUTE

JULY 2025

Special Report

About the author

Chris Taylor is a senior national-security official currently on long-term leave from the Australian Government. Chris heads ASPI's Statecraft and Intelligence Policy Centre, where his research includes emergent and emerging issues facing intelligence services internationally and in Australia, the place of intelligence agencies in democracies, and the role of intelligence in the conduct of statecraft. The author's views as expressed in this report are the author's alone and do not represent those of the Australian Government or any government agency.

Acknowledgements

Sincere thanks to the 28 serving and former national-security officials, industry figures and commentators who shared their views with this project. Particular thanks to Danielle Cave, James Corera, Rochelle Fittler, Brett Greenshields, Raelene Lockhorst and Kyle McCurdy for their contributions to this report.

ASPI would like to acknowledge PentenAmio's sponsorship and support, without which this report would not have been possible.

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.

About Special Reports

Special Reports are written by both internal and external authors, they are intended to deepen understanding on critical questions facing key strategic decision-makers and, where appropriate, provide policy recommendations.

Cover image: iStockphoto/Kirill Smyslov.

Match-fit for the global contest?

Innovation, leadership, culture and the future of Australia's National Intelligence Community

CHRIS TAYLOR

JULY 2025

ASPI
AUSTRALIAN STRATEGIC POLICY INSTITUTE

Special Report

First published July 2025

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
Email enquiries@aspi.org.au
www.aspi.org.au
www.aspistrategist.org.au

Facebook.com/ASPI.org

@ASPI_org

Contents

Executive summary

The business model of the Australian national intelligence community (NIC), including the ways in which the NIC collects intelligence, analyses that intelligence and then provides it to busy senior customers, is being challenged. At the heart of that challenge lies the NIC's relationship with innovation and its ability to take advantage of the opportunities that innovation can bring.

Innovation matters to Australia because our ability to leverage it will be critical to overcoming Australia's 'national capacity' problem in the coming decades. This problem isn't new. Australia has always had an inverse relationship between its extensive geography and interests, and its relatively small population. But that's being exacerbated by the emergent international (and existential) contest in which we're now engaged and the rapid advances of critical and emerging technologies. The answers to this national capacity problem necessarily involve technology, partnerships—and innovation.

Reinvention is hard for all sectors, but it's particularly hard for intelligence communities, which operate with such high degrees of secrecy. But, to keep pace with larger partners and to keep ahead of adversaries, innovation is absolutely essential. It's needed so the NIC can develop more sustainable and creative ways to serve its customers, and the NIC also needs to fundamentally, and continuously, rethink the value it provides to them. Despite growing investment, all intelligence communities can struggle to reinvent themselves—and invest in the right capabilities and technologies—as they deal with multiple global conflicts and the unrelenting pace of change.

In order to inform the findings and recommendations contained in this report, ASPI conducted a range of semistructured, qualitative interviews with 28 former and current Australian national-security officials, industry representatives, and those with comparable experience of the UK's national-security system. The interviews focused on the topics of leadership; technology; risk and experimentation; culture; partnerships; and public engagement and transparency.

This report makes five key recommendations (see page 6), including in relation to actively promoting the concept and practice of 'intelligent failure' in the service of innovation; incorporating an appreciation of the impact of secure workspace design and operation on the effectiveness of the work carried out within those spaces; expediting the 2024 Independent Intelligence Review's own recommendations in relation to national-security technology; an urgent, classified audit of Australia's sovereign intelligence capability resilience; and preparation of the NIC for the impending (and different) future of intelligence production.

Introduction

ASPI's broad stakeholder engagement and 28 interviewee responses indicated that, while there's much that should be praised when it comes to the NIC and innovation—including positive developments like the NIC's Top Secret Cloud project[1] and (outside the NIC) the state of public–private cooperation on AUKUS[2]—there's also much more that can be done.

This isn't surprising. In 2025, technology is the centre of gravity of national power, not just military might—or indeed national intelligence power. It's decisive—not just in terms of advantage on the battlefield or in the shadows—but in economic competition. That includes driving national productivity. At the same time, of course, any Australian Government has multiple competing funding demands; currently, that includes the National Disability Insurance Scheme, supporting an ageing population and an objective of lifting defence spending. At the same time, our threat environment is worsening. As both sides of politics acknowledge, it's at its most dangerous for Australia since World War II, with overlapping and cascading conflicts, crises and tensions.

Consequently, innovation is vital not just to keep up with shifting and increasingly more capable adversaries, but also to do more with less—including making the best use of both in-house and external sources of advice and analysis. Innovation is relevant to attracting, keeping and enabling Australia's most important national-security capability:

its people. Expectations of national-security employees are evolving, and their ways of working are being transformed by technological possibilities (which can be constrained by security requirements).

Innovation in intelligence capabilities is enabled principally by technological advances and tools that are largely created by the private sector. That's a paradigm change from the 20th century. As international contest evolves, and old certainties underpinning Australian capability decisions waver due to a mercurial US administration, the Australian Government will be required to take on a more active role in determining appropriate levels of sovereign capability.[3] Some select 'core capabilities' may actively acquire a capacity for self-reliance or at least new expectations in relation to supporting and directing our national-security industrial base.

But success or failure in innovation for intelligence agencies isn't simply, or even largely, about having the right tools. The primary factors in deciding success are—and will be:

- culture
- leadership
- workforce
- knowledge and learning
- organisational structures and environments
- collaboration and communications.

And, fundamentally, the NIC will need to rapidly develop an improved approach (in spirit and application) to accepting risk and applying experimentation.

Whether Australia's intelligence agencies can master those factors—supported, encouraged (and indeed even cajoled) by ministers and senior policymakers—will be key to meeting future challenges. That includes the challenge of next-generation intelligence production. While consciously avoiding perverse incentives for 'innovation by workarounds' (especially with regard to mobility—as evident in 'Signal-gate').

Methodology

The data collection for this survey was a first of its kind for Australia. In April and May 2025, ASPI undertook 28 semi-structured, qualitative interviews with former and current Australian national-security, intelligence, law-enforcement, defence and foreign-affairs officials, as well as industry representatives and people with comparable experience of UK national security, in order to gauge the present status of innovation in the NIC and help guide policy problem definition and future solution design. Interviewees included former agency heads and deputy departmental secretaries, other current and former national-security leaders, and technical specialists (including those with experience inside and outside government).[4]

More particularly, this project sought to use the wide-ranging interviews to:

- gauge the current status, needs and ways forward for innovation, and understand how Australia's intelligence agencies currently approach innovation
- test those insights against some particular cases of opportunity and threat represented by changing technological and workplace expectations of employees (and how those run up against security requirements) and evolving product requirements for intelligence agencies' customers (as information consumption patterns are transformed by technology), as well as the cautionary tale of the US 'Signal-gate' scandal (and what it has to say about 'innovation by workarounds')
- compare aspects of the Australian experience to that of the UK, given the UK's close connections and institutional similarities with Australia's intelligence agencies
- provide Australian industry with a sense of the NIC's approach, including on the priority accorded to sovereignty in capability development and acquisition, to improve future dialogue and collaboration with the NIC
- identify practical outcomes for intelligence agencies and future opportunities for focus and additional research.

Participants' responses to specific questions,[5] and broader comments, were considered in the context of the recently released 2024 Independent Intelligence Review (IIR) findings and recommendations. Project analysis was also supported by available literature on innovation, including particular applications to intelligence organisations and bureaucracies.

Recommendations for the Australian Government and the NIC

Recommendation 1: Intelligence agencies should incorporate the categorisation and findings from this report on factors influencing innovation success and failure into future planning and evaluation, including by:

a. developing internal policy advice and communications to actively promote the concept and practice of 'intelligent failure' (advancing long-term problem solving through experimentation, including through unsuccessful experimentation)[6] in a national-security context

b. in order to 'look up and out',[7] embracing a purposeful permeability between agencies and between the private and public sectors—at both organisational and individual levels; for example, by making demonstrated experience across government (or in the private sector) a prerequisite for promotion to the Senior Executive Service (SES) within the NIC.

Recommendation 2: In designing and operating secure workspaces, Australia's intelligence agencies should consider not just the security and amenity of those spaces, but also the impact of that design and operation on the effectiveness of working within them (and thus staff morale).

Recommendation 3: The Australian Government should quickly implement relevant IIR recommendations in relation to national-security technology (that is, recommendations 36 and 37) with new funding, given the necessary costs and complexity that would be involved in:

a. 'scop[ing] the establishment of a national security focused technology fund' (in emulation of the UK's National Security Strategic Investment Fund)

b. the NIC developing 'a technology strategy to articulate the enterprise-level vision, requirements, priorities, and risks regarding the current and future technological environment'.

Further to the IIR's recommendation, the technology strategy should consider the shared needs of Australian industry, particularly small and medium-sized enterprises (SMEs), including in relation to opening up opportunities for procurement and investment.

Recommendation 4: The Office of National Intelligence (ONI) should lead an urgent, classified audit of Australia's sovereign intelligence capability resilience and identify particular points of vulnerability.[8]

a. This should be complemented by mapping Australia's national-security industrial base, including in collaboration with the Department of Industry, Science and Resources, following post-election machinery-of-government changes regarding economic security and sovereign capability.

Recommendation 5: Intelligence agencies, led by ONI (and drawing on assistance from outside government), should expand on IIR recommendations in relation to future intelligence delivery to more generally prepare the NIC for future reinventions of intelligence product, such as the incorporation of artificial intelligence (AI) into customer interfaces, to meet evolving customer needs and information-consumption preferences.

What is NIC innovation?

As a former senior technical adviser to multiple Australian intelligence agencies warned in their interview: 'Everyone loves innovation. No one says it's not good. But few really understand what it means or entails.'[9]

Indeed, beyond its deployment as a buzzword, what does innovation mean? Its common usage is to 'introduce novelty' or 'make change': a state of difference from what has been. Or, as journalist Matt Ridley explains, innovation means:

> [f]inding new ways to apply energy to create improbable things, and see them catch on. It means much more than invention, because the word implies developing an invention to the point where it catches on because it is sufficiently practical, affordable, reliable and ubiquitous to be worth using.

Ridley also cites Nobel Prize-winning economist Edmund Phelps's definition of 'a new method or new product that becomes a new practice somewhere in the world'.[10]

Such vernacular definitions have been refined and updated over the past decade, not least as a result of the 'Lean Startup' movement—and the idea of innovation as the fundamental de-risking of a particular business model, and the development of the discipline of 'entrepreneurial innovation'.[11]

There is in fact an international standard for innovation and 'innovation management' (the ISO 56000 series), including the definition of the term 'innovation' as a 'new or changed entity, realizing or redistributing value,' where there is an outcome (product, service, process, model, method, etc.)—and where a particular emphasis is placed on that notion of value (including to distinguish innovation from mere change or 'innovation theatre').[12]

Nonetheless, this project did not seek to impose a narrow definition on interviewees. Rather, interviewees were asked to consider it more broadly as the purposeful adaptation of ways of working, organisational conceptions and approaches, as enabled by technology and within a national-security context.

Indeed, interviewees used and explained their own definitions and characterisations of innovation, as applied to their experiences. One former agency deputy described three intersecting circles of innovation, each requiring careful cultivation:

- innovation for decision advantage (operational innovation)—to be faster, more accurate, more impactful than adversaries
- innovation for capability—with a continuous cycle of planning, deployment and evaluation
- innovation specifically directed at developing and leveraging one's workforce.[13]

An agency senior, currently leading whole-of-community capability efforts, described the componentry of innovation in intelligence agencies as consisting of 'technical and process solutions', 'scanning of the environment / introspection' and 'culture'.[14]

Some interviewees emphasised just how integrated innovation is in their agencies' day-to-day operations and capability development—to the point where distinguishing it as separate was unhelpful.[15]

Importantly, interviewees did distinguish innovation from simple improvement. One industry leader was adamant that innovation 'is not incrementalism; it's more fundamental'. Pointing to a literal cupboard of once cutting-edge but now superseded devices, he described innovation as inherently disruptive, indeed purposefully destructive. True innovation generated approaches that were completely different from the *status quo*. For example, applying AI to cybersecurity—generating dummy decoy networks to divert and defeat intruders—fundamentally reconceives the very logic of cybersecurity (away from static 'walls' towards organisational learning and adaptation).[16] A former intelligence agency senior executive echoed that view, describing innovation as 'reimagination, not iteration'.[17]

Interviewees also contextualised innovation, both to the particular requirements of the public sector and more specifically to national security. One noted that, even in the absence of profit drivers, innovation must contribute to a clear objective;

that is, 'it cannot be valuable in and of itself.'[18] Another, a former senior technology adviser, raised the confronting point that 'innovation is mostly about failure'[19]—a notion that challenges common perceptions of innovation as a linear path to success.

Others drew on comparisons from fields beyond national security. In describing how intelligence agencies grapple with adaptation, one interviewee drew on a novel analogy to the theory of 'punctuated equilibrium evolution' and its sudden, unpredictable bursts of rapid evolutionary change;[20] meaning that agencies must be agile, responsive and comfortable with uncertainty—something for which many bureaucratic structures aren't well designed.

As colourful as they were, the variety of the descriptions above, as offered by interviewees, does suggest more limited understanding of modern innovation practice and theory than might be expected, along with a lack of a clear and shared methodology.

Feedback emphasised that innovation isn't simply applicable to practices or operations but also applies to organisational conceptualisation. That's also clear from the modern history of intelligence. Intelligence organisations have adopted otherwise novel roles to meet government exigencies (for example, the CIA's development and deployment of aerial reconnaissance and then satellites in the 1950s and 1960s), shifting focus substantively to a new domain (as in the shift since the 1990s of global SIGINT[21] efforts to computer networks and then to the digital domain), or reinventing their offering when their historical function had been undercut by commercial enterprise (as in the case of geospatial intelligence in the face of Google Earth).

Why contest means that innovation matters more now than ever

As the IIR notes, ongoing shifts in global power have been 'accompanied by a sharp contest between nation-states for power and influence. This contest is at once diplomatic, military, economic and technological, and is pursued within Australia's borders as much as beyond them …' Furthermore, this contest is 'deeply rooted and structural in nature. It is a feature of the era, not a passing moment.'[22]

That contest strongly influenced interviewees' thinking on innovation.

A former agency deputy noted that Australia is confronting an existential threat environment, and that a key domain of this contest is the information environment, in 'which our adversaries are trying to reduce the integrity of our information inputs, erode our truth base and poison information flows to deceive and deny decision-making'.[23] This is of fundamental importance for intelligence agencies—institutions whose primary purpose is the acquisition and leveraging of knowledge for advantage in decision-making!

One former official was moved to note that current developments in technology (such as ubiquitous technical surveillance and AI) threaten the very viability of national intelligence as an enterprise—and that, without concerted effort to adapt, Australian intelligence might be a particular casualty:

> [A senior foreign intelligence officer] said that there are only going to be four or five intelligence agencies in the world who will survive digital transformation, by being able to dominate in the information space … Australia is also in this race, but is significantly underpowered and smaller than the other runners.[24]

Another former official was conscious that Australia's circumstances might demand hard-headed self-appraisal: 'Are [we] playing to win? Or just not to lose? Playing alone? Or needing to play better as part of a team—not just across national partnerships, but with international and like-minded partnerships?'[25]

The contest isn't confined to geopolitics alone. One interviewee pointed to the emergent contest between states and the heightened, global capabilities of transnational serious organised crime (TSOC). It's no longer only the most

dysfunctional states that can be outmatched by criminals. In fact, increasingly 'unconstrained' TSOC actors are now able to exploit globalised societies and economies (and cross-overs with adversarial state actors) to seriously challenge national security.[26]

Several interviewees identified a fundamental 'national capacity problem' on Australia's part, for which the only answers are technology, partnerships—and innovation. In short, Australia's small population (relative to our broader region) and declining relative national income mean that this contest can't be won through 'quantity' alone—and that long-held assumptions about a qualitative advantage, based on unique access to technology and capital, are increasingly in doubt.

As an industry leader observed, we can no longer 'constrain' ourselves; 'we don't have that luxury'. In this contest, Australia can't afford to 'fight fair!'[27]—a sentiment echoed by others.[28] One serving official pointed out that Australia's intelligence agencies needed to realise that, for the first time in our history, we would soon be 'underdogs'—and underdogs must 'scrap and adapt to survive'.[29] One technical specialist pointed to the application of AI (and its promises of speed and agility) to operational models of intelligence (both collection and analysis) as a critical means of addressing this capacity problem.[30]

Former officials highlighted what they took to be an evident 'knowing–doing gap' emerging within the Australian Government, characterised by a gap between the existential rhetoric deployed by ministers (in both the current and previous governments) and seemingly slow responses by national-security institutions (noting public criticism of Defence in this regard).[31] Others worried that the recent federal election's apparent endorsement of a wider *status quo* in Australian policy (and its impact on contestability and the generation of new ideas), might entrench that gap.

Outside of the intelligence community, one former senior ADF officer diagnosed the specific 'gap' in the defence space as a 'missing middle' within the Defence bureaucracy, which continues to proceed on the basis of 'business as usual': 'the troops get it, the politicians get it, "Russell" doesn't get it.'[32] A former senior intelligence officer identified 'policy sclerosis' across the broader national-security bureaucracy and blamed structural factors within government but also poor public-sector leadership, wedded to superseded assumptions.[33]

It was clear from the discussions that the contest in question is only being further complicated by recent developments within the US Government and in US policy internationally. As I've noted previously,[34] Australia has no room for complacency as it watches the second Trump administration up-end the US intelligence community (USIC). The evident mutual advantages of the US–Australian intelligence partnership and of the Five Eyes alliance more generally aren't enough to guarantee the preservation of related benefits. This is requiring the NIC to adopt a more deliberate and coordinated approach to its relationship with the USIC, centred around agreed national objectives. Past certainties, including those upon which Australian capability planning has rested (for example, that sourcing capability from the US was not meaningfully different in terms of risk from sourcing it domestically), no longer seem so certain, and that conclusion extends beyond the NIC to Australian national security more broadly.

However, a positive note was struck by several interviewees; namely, that there was now an opportunity to act in response to these changes—before crisis strikes and those assumptions are found wanting.[35] Indeed, as one respondent noted:

> There is a gold window of opportunity for us to partner and put in place the security operations/opportunities for the coming decades.[36]

Other interviewees, especially from within the NIC itself, expressed confidence in current interdependencies, pointing to past and present (and anticipated future) capability advantage through Australia's close international relationships, especially within the Five Eyes alliance.[37]

What's determining successful innovation in the NIC?

Given the evident imperative for innovation occasioned by the conditions of contest, what factors are central to success and failure in the intelligence context? And how is the NIC challenged to evolve its approach to innovation and master those factors?

As with the definition of innovation, interviewees were given the latitude to identify and evaluate their own relevant factors. Some provided a general critique of current approaches to innovation, citing 'fear of disruption', 'preference for established methods', 'institutional conservatism' and 'lack of awareness and training'.[38] Others offered a pithy summation of the keys to success: 'courage, change and culture'.[39]

More broadly, the responses provided by interviewees on success and failure in intelligence innovation can be categorised as follows.[40]

Culture

Almost all interviewees highlighted the importance of culture, and in fact there is a cultural dimension to each of the subsequent factors identified. As a former diplomat noted, '[T]he biggest hurdles to adopting innovation are cultural and until you address cultural resistance, nothing will change.'[41]

This included a general emphasis on encouraging collaboration and diverse perspectives and insights. Curiosity was prized.[42] And for one former agency head what was most critical was a workforce's 'particular hunger for the next thing, the next success, the next advantage'.[43]

Despite well-publicised issues concerning past events on deployment in Afghanistan, several participants waxed positive about the current culture within Australia's special forces, highlighting the special forces' embrace of an innovation culture as more positive than their experiences either within the NIC or in Defence proper.[44] This included the specific features of:

- independent funding lines, with decision-making as close as possible to the problem and the expertise
- skilled practitioners committed to constant learning
- trust and risk appetite
- focus on outcomes.[45]

Another interviewee pointed to their international experiences, comparing what they saw as a stifled innovation culture at home with that of their former Iraqi counterterrorism colleagues. On reflection, they identified the more innovative approach of the Iraqis as grounded in:

- a culture of creativity—and having to make do
- the imperative of winning the war against the Islamic State of Iraq and Syria (ISIS)
- a literal sandbox for experimentation.[46]

One respondent identified a key barrier to effective collaboration—and therefore innovation—as the development of cultural arrogance within and between agencies, often stemming from profound misunderstandings of each other's roles and work. It was necessary for agencies, and the NIC as a whole, to be alert to this tendency—as universal as it is in all organisations.[47]

One close observer of the intelligence community directly linked existing organisational culture (and workforce selection and training biases) to risk aversion (see below), explaining that:

> From walking into [the intelligence community] we're led—unconsciously—to see innovation as tantamount to risk. At an operational level it's the template, the [standard operating procedures] that are drilled into us.

> We don't do what we should do—imbue that initial understanding with the idea that innovation is what we actually do; it's what our forebears did, and what our successors will do.
>
> Yes, rules are important. But we end up building a 'cultural box' and telling people how to behave within it.
>
> Of course, we don't want unnecessary risk takers, but selection for dutifulness does have negative effects on (constructive) creativity.[48]

That same observer identified his own checklist for the ideal innovation culture for Australian national security as:

- curiosity
- humility
- perspective
- difference
- diversity
- imagination.[49]

A serving senior officer noted the difference in change-mindedness between the intelligence community workforce and their private-sector counterparts arising from the necessary pattern of technology change within intelligence agencies (staged, careful, irregular) compared to the private sector (a constant tempo, conditioning acceptance of constant change).[50]

Leadership

A related success factor is leadership. It featured prominently in responses, and interviewees were eager to explore how it could most effectively support successful innovation. One former deputy agency head identified leadership as key to adopting a contest 'mindset', by focusing on robust net assessments of our own strengths and weaknesses in addition to those of adversaries.[51] In fact, humility was mentioned by several interviewees as key to effective leadership of innovation. As one change specialist observed:

> Maybe you're not the smartest person in the room and that isn't a problem. It is a problem if you're focused on proving you are! Have the intellectual maturity to ask others how can we do better—and who can help us do that? Otherwise, … you end up stuck in premature solution identification, leapfrogging proper problem identification.[52]

Or, as another respondent remarked of the 'new' requirements of leadership: 'Listen more and speak less.'[53]

But humility isn't enough. Successful leadership of innovation requires a commitment to acquiring and sustaining a technology literacy commensurate with today's environment. A former senior technology adviser warned that otherwise agency leaderships can't effectively evaluate and decide, and 'end up accepting things that you shouldn't', including sub-optimal technical outcomes.[54] This should be expected throughout the SES, the members of which should not only be 'tech literate but tech ready'.[55]

Underpinning this commitment are the twin requirements for leadership of curiosity and contestability.[56]

Another respondent argued for leadership to 'centre people' and, interestingly, observed that in their view Defence was more successful at this than intelligence agencies, given its responsibilities to others arising from putting subordinates in 'harm's way'.[57]

A similar observation about centring people has been made separately by former UK Government Communications Headquarters (GCHQ) Director Robert Hannigan:

> In short, this was a leadership that could live with tension without feeling compelled to resolve it immediately. In holding that tension, it resisted the natural tendency of any organisation to homogenise, standardize and dilute. Here were leaders who did not feel threatened by staff more expert and brilliant than they were, leaders who were self-effacing and verging on the reluctant. At their best, they embodied the paradox of this secret world. By understanding and prizing people above technology, they enabled the greatest technological advances imaginable.[58]

For some, what was a key to innovation success was a leadership's ability to make difficult decisions, especially around forgoing legacy systems (or ways of working) in order to progress and improve.[59]

There was also discussion of how to create incentive structures to generate leadership geared to innovation success. One interviewee criticised current incentive structures for not aligning with new leadership needs:

> [W]e don't reward people for stepping outside of their lane, their agency. Nor for displaying the attributes I've cited. We tend to reward—consciously or not—bravado, action, decisiveness.[60]

Those unconsciously rewarded behaviours are in fact the opposite of what best serves innovation, including the fox-like thinking (curious, sensing, restless) prized in agile methodology.[61] Or, as a survey participant explaining their own preferred approach put it:

> The other analogue … is being like a detective. Proving [a] fundamental hypothesis from the ground up, building an evidence base and being impartial, able to be led by the data. This should be easy for people in the NIC, but is contradictory to a lot of common leadership behaviours.[62]

Another highlighted former CIA Deputy Director Carmen Medina's comments about the power of transcending ego:

> [Y]ou have to make your idea somebody else's idea. You need to make your idea community property … What should I do when somebody else gets the credit for my idea? And our answer is 'celebrate'.[63]

A former agency head pointed to the value of engagement between intelligence agency leaders and exemplars of innovative thinking within the broader Australian Government (such as CSIRO's Data61 Business Unit) to encourage emulation and borrowing of ideas (and make intelligence agency leaders conscious of any relative lack of ambition on their own part).[64]

Risk and experimentation

A further success factor is the approach adopted to risk—and, by association, experimentation. This was a consistent theme of interviewees' responses to the question of what influences success and failure in innovation. Surprisingly, given that the *raison d'être* of national-security agencies (especially intelligence agencies) is effective engagement with often very significant operational risk, those responses often identified non-operational risk aversion as common in the NIC.

Interestingly, a landmark 2021 examination of innovation in the USIC similarly concluded that:

> … decision making remains too focused on the risk of action but fails to assess and incorporate the risk of inaction and the opportunity cost of not acquiring and integrating new technologies into intelligence missions. This task force does not cavalierly dismiss the critical threats and risks … associated with new technology and data streams. Indeed, risk must always be central in analyzing technology adoption, but decisions cannot be made solely on those grounds. An element of [US]IC culture that leaders must prioritize transforming is this risk aversion, where risk-taking, experimentation, and creation will be rewarded and where innovators are not unduly punished when there is inevitable failure.[65]

Many interviewees felt that risk aversion was a significant brake on national security, although not all agreed that the risk aversion was principally an agency problem. Several former senior intelligence agency staff sheeted home responsibility for such aversion to top-down cautionary signals from ministers and senior departmental officials.[66] Others traced the aversion to signals within agencies; one commented that 'under present circumstances, no one is punished for going too slow. But you can be punished for going too fast.'[67]

Still others raised the issue of what they perceived as an increasing misalignment between expertise, decision-making and risk within organisations, often associated with significant and rapid growth. The greater the distance emerging between grounded technical expertise (often at EL1 and EL2 levels) and actual decision-making on technical issues (at the SES level), the less confident decision-makers became and the more they erred towards caution.[68] And the less experienced in directly dealing with risk those more junior officers become, compared to their predecessors who, in smaller organisations, were sometimes responsible for significantly expensive programs.[69]

Some pointed to a tendency in larger national-security organisations (including Defence) for decision-making to quickly 'go wide', drawing in ever more tangential stakeholders, ultimately leading to the same safety of the *status quo*.[70] An experienced engineer explained his own analogy for this effect, based on the failure of collective action by people in a metaphorical room to turn on a light when the room is unexpectedly darkened:

> The … room is always filled with people asking 'Can we do this?', never with people asking 'How can we do this securely?'. The more voices in that room—who are not engaged in the solution—the more stymied innovation becomes.[71]

Alternatively, one serving senior officer located the most challenging risk aversion as arising from middle management ranks where a lack of self-confidence could lead to self-censorship of ideas.[72] A key to overcoming that was, according to others, meeting the challenge of conceptualising experimentation in the national-security space (and an understanding that this can be achieved with suitable guardrails) but also embracing the idea of 'intelligent failure'—especially in dealing with challenges where not only the answers are unknown but the very questions being asked are unavoidably unclear. Incentives are critical here. As one former intelligence officer explained, too narrow a focus on specific outcomes could produce perverse results:

> We reward dumb luck. The equivalent of the drunk driver who makes it home safe. We punish intelligent failure—even when the decision-making was right, although the outcome wasn't what we hoped for.[73]

Such 'un-acceptance of failure' can lead to either 'big "successful" programs that are meaningless' or—more dangerously—'agile processes but a (very dangerous) culture that won't allow reporting of bad news', according to an industry observer.[74]

Regardless, as one former senior intelligence officer pointed out, any successful embrace of risk and experimentation requires agreement on 'where and what we're willing to risk'. The same ex-officer highlighted, as a useful model for intelligence agencies to emulate, the Australian Government's emerging approach to AI risks (in which, for example, a domain such as health might require a more constrained risk approach than in other domains).[75] The potential enabling role, in this regard, of risk appetite statements in the broader Australian Government has been highlighted elsewhere.[76]

Several current intelligence community leaders pointed to continually improving approaches to risk and innovation within their agencies. In one instance, this drew on the insight that their organisation would need to 'risk to de-risk', in which the application of novel data techniques (including the deployment of AI tools) was vital to identifying otherwise obscure threats and leads hidden in vast information holdings.[77] In another instance, an agency sought to use its relatively small size and limited resourcing to embrace a proof-of-concept approach to innovation that allowed for steady progress and the opportunity to prioritise capability development more effectively.[78]

(Self-)knowledge and learning

In expanding on their responses concerning both culture and risk, several interviewees highlighted the requirement for self-knowledge (at both individual and organisational levels) and the availability of systematic approaches to learning as a critical factor. In fact, one former intelligence officer described learning as 'an insurance policy for experimentation', ensuring that failure could indeed be intelligent.[79]

Self-awareness and learning are also important in implementing change. One industry figure gave the example of the introduction of secure mobility solutions into a military headquarters in an exercise environment (see box). The optionality provided by the new communication tools, including to significantly optimise the headquarters' ways of working, was not enough. Instead, mobile systems were just moved from stationary workspace to stationary workspace.[80]

Secure mobility: background

Secure mobility is the ability to access and share sensitive data securely while on the move—across devices, locations and networks—without compromising classified or protected information. In national-security and defence contexts, it typically involves:

- encrypted communication tools
- secure mobile devices and platforms
- controlled access to classified networks
- real-time data sharing in the field
- protection against interception or cyber intrusion.

Workforce—and accommodating constructive disruption

A number of interviewees expressed concern that more wasn't being done to encourage a more diverse, including neuro-divergent, workforce. Some pointed to related characteristics having historically been a source of comparative advantage, especially in more technically engaged organisations.[81] This was accompanied by concern about a loss of emphasis on developing and sustaining expertise in favour of generalism, and a perceived decline in the ability of organisations to effectively use disruptive but constructive experts:

> Expert voices are often absent [in decision-making]. If they are present, then they're strictly advisory. Of course, that expertise can't be too narrow. It needs to be suitably rounded, confident. But the kind of voices we're talking about are often disruptive, and organisations need to work out how to accommodate them. [My former agency] used to be much more embracing—not just tolerant—of these disruptors.[82]

Although the same observer cautioned against too-nostalgic looks backward:

> What was possible in the late 1990s with just some clever people (which led to amazing capabilities) is no longer possible.[83]

Environment and organisational structure

Interviewees were asked how, in their experience, organisational make-up and structure aids or impedes innovation. As with the impact of enhanced resourcing, there were differing views about whether scale helped or hindered innovation. Some believed that it was counterproductive due to increased bureaucratisation[84] and even disproportionate growth in senior ranks.[85] Others challenged past claims that the relatively smaller scale of Australian organisations, compared to their allied counterparts, explained the innovation gap; one official dismissed this as a 'crutch'.[86] A serving official argued that the direct relationship between rising technology costs and increasing capability benefits inherently advantages scale and punishes smallness.[87]

Interviewees also contemplated the question of where innovation might best be located within organisations; alternative models included the establishment of stand-alone innovation functions and innovation as 'everybody's business'; in a sense—pedestal or coalface.

There were those who argued for location as close as possible to the problem to be resolved.[88] One former official argued that 'If it has "innovation" in its title then it's by definition too far away from the business and will fail,'[89] although others emphasised the advantages to innovation from a more centralised innovation element's greater proximity to resources, time and leadership focus.[90]

Perhaps the best description of the 'goldilocks' position that best reflects contemporary best practice in industry (and helps avoid 'innovation theatre')[91] came from a serving senior official who noted that an organisation's 'core' needs to own that organisation's innovation framework, so as to help the rest of the organisation generate—and, importantly,

implement—ideas, because innovation needs to be at least a slice of every employee's work. That core needs to be backed with systems to capture/filter/track innovation and ideas, and the core's staff need to carry suitable authority applicable across the organisation. This includes the organisation embracing the choice of devoting these experts/achievers—including associated opportunity costs. Critical to making this balance work is openly demonstrating resulting wins and outcomes within the organisation.[92]

A version of this arrangement was adopted successfully at one of Australia's largest intelligence agencies, where an empowered senior technology adviser reporting directly to the agency head provided initial organisational 'horsepower' to generate the take-up of innovation, but all SES staff were expected to be responsible for innovation in their respective functions.[93] That arrangement has since evolved towards one in which that horsepower has been normalised within the division responsible for technology.[94]

Some interviewees pointed out that there's also an important structural dimension to contestability and risk, arguing that contestability needs to be systematised within organisations. It can't rely simply on personal leadership and encouragement.[95] Others pointed out that the same structure also needed to effectively collectivise calculated risk, rather than letting it fall on the shoulders of individual leaders and staff.[96]

'Community' and interagency relationships

By contrast to some of the reflections on innovation within intelligence agencies, the tenor of responses about how the NIC works as a cross-agency innovation community was generally (although not uniformly) positive. The positivity included observations about the innovation benefits to Australia arising from the expansion of the CIA-originating In-Q-Tel innovation network to Australia and the UK—acting as a bridge between government agencies and innovative tech start-ups and accelerating the adoption of cutting-edge solutions.[97]

A number of interviewees highlighted the valuable work of the NIC's Innovation Hub (itself an outcome of the 2017 IIR, led by ONI and aimed at fostering innovation through collaboration between government agencies, academia and industry partners), including its work in identifying national-security technology needs across intelligence agencies and matching those needs with technology available or in development from industry.[98] As one former official, now engaged in industry explained:

> ONI's Innovation Hub is doing an increasingly good job. Great model, and the key change has been staffing it with good people. Still too small, but it's proving it can overcome NIC cultural suspicions.[99]

However, it was also clear from discussions that agencies are still not taking full advantage of the hub, despite its outreach, and there remains a danger that the hub's particular value in seeing beyond the technology horizon might be crowded out by more immediate-term requirements (that agencies themselves are probably best placed to address). There's also a natural tendency for the Innovation Hub to be drawn towards flashier but more speculative high-end operational 'possibilities' at the expense of proven opportunities in relation to foundational enterprise systems—including organisational learning.[100]

Another gap, and an opportunity for innovation enhancement, was intelligence agencies' engagement with the rest of government—including with the states and territories (which have their own innovative capability programs underway, notably for law enforcement).[101]

Public engagement and transparency

Several interviewees focused on enduring difficulties in the intelligence community's approach to public engagement and transparency, and how those issues affect national-security innovation. Several industry figures specifically mentioned the absence of ready engagement points for smaller firms seeking to establish relationships with the NIC or to offer new tools and services that might be useful for intelligence agencies.[102]

Other interviewees noted enduring challenges for intelligence agencies in effectively articulating those agencies' capability requirements, especially (but not only) where those requirements are linked to sensitive operational equities. This poor communication includes agencies being too quick to demand specific solutions instead of clearly defining the problems they need to solve, often resulting in sub-optimal outcomes.[103]

That opacity also has a detrimental effect on the ability of intelligence agencies to benchmark their capabilities against others (especially beyond close allies). As a technologist with extensive national-security experience remarked: 'It's a bit like believing you're the fastest runner in the world because you've only ever seen races at your primary school.'[104]

One suggested means of improving communications between intelligence agencies and the private sector was raised by an interviewee, who highlighted the suggestion in the 2017 IIR for an annual, differently themed, conference in this regard that would bring together agencies and industry.[105]

Other factors

Other factors identified by interviewees that contribute to success or failures in innovation across the NIC included:

- a need for *pragmatism* in balancing innovation with addressing technological fundamentals, and especially the sustainment of systems and their life cycles,[106] including using the 'explore versus exploit' model to help maintain a balanced portfolio of work[107]
- metaphorical and literal *space* for innovation, often as a higher priority than access to novel technologies[108]
- practical difficulties associated with a 'case by case' approach to *security accreditation* of new technologies, associated expenses (especially for smaller firms), and a requirement for agreed government sponsorship (the 'chicken and the egg' conundrum)[109]
- the necessity of giving innovative disruptors within agencies the necessary time and licence to make things happen—estimated by one senior serving official as approximately five years.[110]

Recommendation 1: Intelligence agencies should incorporate the categorisation and findings from this report on the above factors influencing innovation success and failure into future planning and evaluation, including by:

a. developing internal policy advice and communications to actively promote the concept and practice of 'intelligent failure' (advancing long-term problem solving through experimentation, including through unsuccessful experimentation[111]) in a national-security context

a. in order to 'look up and out',[112] embracing a purposeful permeability between agencies and between the private and public sectors—at both organisational and individual levels; for example, by making demonstrated experience across government (or in the private sector) a prerequisite for promotion to the SES within the NIC.

Future challenges to (and opportunities for) the NIC's approach to innovation

The relatively healthy state of investment in Australian national security (and more specifically the NIC) suggests that resourcing and capacity, often otherwise seen as a constraint on innovation, are less relevant today. Since 2021, successive governments have made transformational long-term additional commitments to agencies—including the Australian Signal Directorate's Project REDSPICE ($9.9 billion)[113] the Australian Security Intelligence Organisation ($1.3 billion) and 'modernisation' of the Australian Secret Intelligence Service ($1.6 billion), each delivered over 10 years. In response to the 2024 IIR, the government has also committed an initial $44.5 million over four years to ONI for initial implementation of IIR recommendations, including for NIC training.[114] Although some interviewees were keen to emphasise just how focused these investments have been on the effective delivery of specific capability deliverables agreed at the onset of long-term transformation programs.[115]

Some interviewees expressed concern that these early commitments to deliverables might ironically act as a brake on innovation, and they encouraged agencies to consciously and deliberately create space for innovation within this 'additional' capacity.[116] That included pointing to examples within Defence in which available resourcing incentivised 'throwing people and money' at problems, with diminishing returns.[117] There was also a recognised requirement for governments, having made these investments on the basis of the expressed need for often fundamental transformation to aspects of the intelligence business, to demand genuine innovation by agencies in response, rather than more of the same.[118]

Leaving aside capacity, there's an argument that there's much intelligence agencies can learn from available business literature about success and failure in innovation (especially in application at the workplace level) and the relative importance of different success/failure factors.[119]

There's also a temptation for the 'distinctiveness' of the intelligence mission, and the unique authorities and responsibilities of intelligence agencies, to lead to a belief in intelligence agencies being *sui generis* in relation to organisation and capability—especially in the technology space. As a result, opportunities are missed to learn from what is common, not only within the public sector but across the broader economy and society. While national security has specific characteristics that limit the direct applicability of external insights and off-the-shelf commercial options, including 'the four horsemen of secrecy, complexity, risk aversion and groupthink',[120] lessons from outside the national-security domain should not be disregarded.

By way of parallel reflection, a recent, unique academic effort to apply such lenses to the particular experiences of intelligence organisations found 'innovation capability' as having the attributes listed in Table 1.[121]

Table 1: The attributes of innovation in intelligence organisations

Attributes	Descriptions
A clear vision and strategy	A cohesive and clear strategy for innovation articulated by organisational leadership
Harnessing the competence base	Organisational processes for channelling resources to innovation
Organisational intelligence	Ability to learn from customers and about competitors
Creativity and idea management	Organisational routines for generating and capturing new ideas
Organisational structure	An organisational structure that allows for innovation processes
Culture and climate	An organisational climate that allows for risk taking and ambiguity
Management of technology	Understanding and absorbing emerging technologies

In this project, four particular cases of opportunity and threat relevant to future innovation within the NIC were explored with interviewees:

- changing technological and workplace expectations of employees (and how those run up against security requirements)
- the issue of sovereign capability for the NIC, amid complex international developments
- evolving product requirements for intelligence agencies' customers (as information consumption patterns are transformed by technology)
- the cautionary tale of the US 'Signal-gate' scandal (and what it has to say about 'innovation by workarounds').

Technology-empowered innovation and Australia's future intelligence workforce

The imperative for innovation in national security isn't just a matter of geopolitics or threats posed by empowered criminal organisations—it also has a human dimension.

As the IIR noted:

> A highly skilled and committed workforce is one of the [NIC's] greatest assets. Sustaining this advantage is no easy task … any erosion of the community's attractiveness as an employer will weaken its ability to manage the high demands of the era, those present and those clearly evident on the horizon.[122]

One example of such erosion is a limitation on mobile technology usage within the high-security work environments typical of Australia's NIC—both for personal use but also for professional uses now common to workplaces in the broader community. This extends beyond access to mobile devices to include security-required lags in the take-up of other technologies, including generative AI. As one former senior intelligence official noted:

> Even when we pull tech tools into classified spaces—they're lesser versions because they don't have the connections and data required to work to their full potential. [This] has become more acute in the last 5–10 years. Especially as cloud computing, neural networks, machine learning have become the norm for tech.[123]

For over 15 years, the question of how technology attracts and retains new generations of 'digital native' staff who have grown up with digital technology as a natural part of their daily lives has been of significant concern in the private and public sectors with regard to the recruitment and retention of talent.[124]

Interviewees were drawn on the question of how security-imposed limitations on technology use affected both the attraction and retention of talent, and effective performance within national-security agencies.

Many interviewees were concerned about a mismatch between technological assumptions about national-security work and its actuality for most employees. As one former senior official remarked:

> [L]ook at who is graduating now. They're actually really smart, connected and naturally collaborative. They have great potential as contributors to national security—and to help reshape traditional ways of working in national security. But they're also disappointed on arrival! They end up thinking 'There was more capability in the phone I left outside than what I'm accessing in here!'[125]

Or, as a former government technical specialist now working in private industry noted:

> After leaving government, and now, having continued engagement with government, I see a continued gap between what is available for commercial use and what is available within government—the innovation gap continues to grow.[126]

A separate interviewee concluded that this gap may develop into a significant barrier to intelligence agencies achieving their ambitious employment goals.[127] For, as the 2024 IIR notes, this is occurring in the context of a tight national labour market but also challenges unique to younger workers in intelligence agencies, including long lead times for security clearances, the preponderance of Canberra-based positions and relative workplace inflexibility.[128] Those challenges will only be exacerbated in the specific STEM space, given reliance in the broader economy on migration to fill skills shortages (and the difficulty of employing many recent migrants in roles requiring security clearances).[129]

Importantly, this isn't just a matter of convenience for national-security staff. These constraints affect the substance of how national-security decision-making works. As the former head of the US Navy's training observed after a spell in similar conditions at the Pentagon:

> By relying on stale slides, we focus on small numbers of carefully selected data points, simple assertions, and bullet-point plans. Nuance and complexity dissolve. Since our conference rooms too have no connectivity, no one brings a computer. Slide decks are not viewed on screens but printed on paper and distributed by hand, with people taking notes with pens and pencils. No one can pull up data to question the assumptions, facts, or conclusions being presented. Everyone is stuck discussing the information the briefers brought to the table, whether it is accurate or not.[130]

This gets to the heart of what the highly capable people found (and sought) in the national-security community want: to matter, to achieve, for their work to be meaningful. Those goals can be aided by technology but also thwarted by its limitation.

As an experienced engineer remarked:

> This is why the kind of innovative, flexible workplace is important. Not so much because it's more comfortable or pleasing, but because it allows better for that achievement. So, for example, if limitations on working (access to information, tools, flexible ways of working etc.) mean that I'm required to continually solve everything from first principles. And I'm not allowed to stand on others' shoulders, as I would be on the outside. Then I might only have one or two genuine successes in my time inside the national-security community. Whereas I might otherwise have multiples of that. This has a real impact on people.

A leading industry figure specifically linked this to the opportunity presented by AI:

> The really significant change at the moment is the integration of AI into workflows—copilots through to AI agents. Critical to making that happen successfully is giving knowledge workers the literal and metaphorical space to do this. And that means unchaining the human from the desk.[131]

Achieving that is also likely to require a reset by agencies that have sometimes undervalued their employees' time, according to one observer. Another former official noted that this undervaluation was sometimes a consequence of efficacious workarounds available to decision-makers but not to their staff. So, in one instance in which innovative approaches to mobility within a high-security environment were being contemplated, the same sense of the requirement for better working wasn't necessarily felt by senior leaders whose needs were already met through dedicated personal staff to produce hardcopy documents, immediate proximity to meeting spaces, and so forth.[132]

Reform in this space is by no means easy. The very real technical security challenges involved in introducing secure mobility in these circumstances shouldn't be underestimated. Indeed, as one serving intelligence agency senior official noted, the logic of 'contest' described above may actually require a rebalancing back towards high-security workplaces.[133] There's also a danger of inadvertently creating two-tier workplaces where some staff have access to these technologies and others, including in more sensitive circumstances, do not.[134]

As the interviewees indicated, there are significant advances being made in some agencies in getting the most advanced technologies to staff, even in high-security environments. That includes where agencies have leaned into providing staff with access to new systems and applications and allowed them to experiment within defined guardrails (and in a safe environment), using the monitored results of those experiments to identify priority future use cases more broadly within that organisation.[135] Other interviewees put the onus for resolving this squarely on agencies, pointing to success in particular organisations.[136]

Recommendation 2: In designing and operating secure workspaces, Australia's intelligence agencies should consider not just the security and amenity of those spaces, but also the impact of that design and operation on the effectiveness of working within them (and thus staff morale).

How sovereign is Australia's innovation-enabling national-security technology, and how sovereign does it need to be?

A related focus of this project's engagement with stakeholders was the interface between intelligence agencies and the private sector that underpins technology-enabled innovation. More specifically: mercurial developments within the US Government since the re-election of Donald Trump have enlivened longstanding debate within Australia about the sovereignty of systems and supply chains, especially in a world dominated by Chinese manufacturing. This isn't because of perceived malice from previously dependable allies, but rather a recognition that even close partners can have differing priorities and demands on 'shared' capabilities—sometimes drastically affecting their reliability.[137]

A number of industry stakeholders described what they perceived as disincentives to the development of an Australian industrial base to meet a significant proportion of Australia's national-security technology needs—including for the NIC. Several perceived that procurement practices and risk attitudes on the part of Australian agencies require that Australian firms, especially at or soon after start-up, seek commercial opportunities with the US Government first (that is, selling to

American national-security buyers) before they could successfully offer their wares to Australia. Many described positively a more pro-SME attitude by US Government customers and an apparent willingness to take a chance on new offerings.

As one successful industry figure lamented:

> [B]oth the US and UK have a procurement psyche that deliberately engages and supports local industry—and its sustainment. They expect that to deliver advantage, and it does. They expect their industrial base to provide their solutions. We expect our foreign partners to do that …
>
> All too often, we [Australia] think we need to see a solution working elsewhere (overseas) before we take it up. It's a shame, but a fact, that the first customer for an Australian product can't be an Australian customer. This is the advice we provide Australian start-ups.[138]

A separate industry leader expressed this in national cultural terms: Australia is 'an acquisition culture rather than a build culture.'[139]

Others tied these issues back to the risk aversion negatively affecting intelligence agency innovation (see above):

> This … extends to procurement, contracting etc. We need to develop different frameworks attuned to national security—and to experimentation—not just templates from the Finance Department. That doesn't mean not asking for value, but it means a different risk calculus, a recognition that in some cases the 'question' will be so important that trying to answer it, even unsuccessfully, constitutes success. Again, what's important is building ways of thinking that find success in such failure, for the next go around.[140]

Although this 'America first' strategy has been deployed successfully by many companies, stakeholders identified two shortcomings. For the eventual Australian agency buyers, it means that technologies originally conceived in Australia are substantively shaped and developed to US Government—rather than Australian Government—needs. And the Australia-originating companies can ironically find themselves caught up in US export controls when attempting to offer their technologies back to Canberra.[141]

Is there a case for 'Buy Australian first'? For some interviewees that was obvious:

> No one in Kyiv or Beijing is having to even have this conversation. It's absurd.[142]

Others made the case that Australian-ness couldn't be a primary basis for procurement in the NIC but that it was necessary for agencies (singularly and collectively) to factor sovereignty into decision-making, including procurement. That might well require a generational change within the national-security bureaucracy.[143] For others, there was a particular case for 'Australia first' with regard to national-security software solutions.[144]

The question of sovereignty also prompted broader reflections by interviewees, including on the differences in approach between Australia and like-minded partners (such as in the UK and Canada). For a number of former senior national-security officials interviewed, there was a sense that longstanding Australian approaches gave Canberra less freedom of movement than London (or indeed Ottawa) in relation to capability acquisition and deployment.[145]

To some, this was reflective of a broader cultural approach by Australia that would need to evolve as long-held certainties about the US weakened:

> This inability to be purposeful and hardheaded about relationships is a national problem as well as a national-security community problem. It's about culture and attitude. Brits are excellent at this. [The] idea of 'only permanent interests' drives their entire apparatus.[146]

One interviewee highlighted, as a distortionary factor for Australian technology capability development, the otherwise benign provision of 'free' capabilities from allies. Too often, those capabilities were only 'free' at the point of acquisition, and were then 'dependent on a whole range of capabilities we don't have and on [additional] resources for sustainment. Then we discover we're chained to a quickly outdated version of that capability, which isn't attuned to Australian needs.'[147]

Importantly, the expressed need for change wasn't about eschewing relationships, including with historical allies. In fact, there was a consistent support among former officials for Australia to actively engage with both Five Eyes partners (beyond just the US) and increasingly close other partners (such as Japan, Korea and Europe) on technology collaboration for national-security purposes. That could include coordinated engagement with tech giants to deliver new solutions that wouldn't be economical individually.[148]

In addition, those more critical interviewees typically made the case for identifying a number of core national-security capabilities that Australia should actively develop and sustain on a sovereign basis, to correct what they described as 'market failure'—with a particular emphasis on the criticality of information delivery. In one example, a technical specialist identified as priorities:

- cryptography (including post-quantum cryptography)
- electronics manufacture
- telecommunications and radio-frequency-related equipment.[149]

A strong counterpoint to these concerns was expressed by currently serving senior intelligence officials, who pointed to the very real capability benefits extended to Australia, especially via the Five Eyes alliance, that couldn't be replicated on a wholly national basis.[150] One noted that the unavoidably small scale of Australian industry, relative to the needs of intelligence agencies, means that:

> [o]ur international partnerships (industry and government) are critical for us. Yes, sovereignty does matter. And we should be being prudent about core capabilities that we need to be assured and reliable always. But that will only ever be a small subset … What's required is a realistic sovereignty.

The same official sounded a note of caution about false autonomy, given the existing integration of national-security capabilities across allies: 'If you really wanted to create a genuinely autonomous ("sovereign") national [intelligence] capability you'd just have to start again—and end up with a lesser result'. It was also unrealistic to compare directly the UK and Australian experiences (and needs). As the official noted, the basis for UK freedom of action extends way beyond questions of particular national-security technologies to broader national capabilities—right up to an independent nuclear deterrent.[151]

In addition, one former official suggested developing a matrix-based model for guiding sovereignty and technology decisions by intelligence agencies:

> [H]ow much control do you need (high or low) versus how specialised or unique is it (high or low) … For something high/high [e.g. sensitive operational technology] this likely needs to be developed in house. For low/low (i.e. laptops or compute power) you can outsource. For low control, high uniqueness [e.g. less sensitive operational techniques] you need to work with close/trusted partners and for high control / low uniqueness (i.e. deniable internet access) you can commercialise with strict project management. We need to be better at understanding what we really need to protect (i.e. build in-house) versus what we can outsource.[152]

One serving official emphasised a perspective that centres Australian expertise as much as Australian technology itself, while recognising their interrelationship:

> AI, quantum and biotech (and especially combination[s] of the three) [are] prime examples of where a lack of in-house expertise threatens to disadvantage us going forward. Not only will we end up less informed price takers, but what ends up available as capabilities will be less compatible with our particular needs (we'll have missed branching opportunities during development). Furthermore, others will have beaten us to the novel applications of these technologies—and we'll be less able to understand them from a defensive perspective.[153]

Recommendation 3: The Australian Government should quickly implement relevant IIR recommendations in relation to national-security technology (that is, recommendations 36 and 37) with new funding, given the necessary costs and complexity that would be involved in:

a. 'scop[ing] the establishment of a national security focused technology fund' (in emulation of the UK's National Security Strategic Investment Fund)

b. the NIC developing 'a technology strategy to articulate the enterprise-level vision, requirements, priorities, and risks regarding the current and future technological environment'.

Further to the IIR's recommendation, the technology strategy should consider the shared needs of Australian industry, particularly small and medium-sized enterprises (SMEs), including in relation to opening up opportunities for procurement and investment.

Recommendation 4: ONI should lead an urgent, classified audit of Australia's sovereign intelligence capability resilience and identify particular points of vulnerability.[154]

a. This should be complemented by mapping Australia's national-security industrial base, including in collaboration with the Department of Industry, Science and Resources, following post-election machinery-of-government changes regarding economic security and sovereign capability.

An innovation opportunity: meeting the needs of the next generation of intelligence consumers

The value of intelligence ultimately hinges on its consumption and appreciation. Regardless of how exquisite or audacious an operation might be, or how penetrating an analysis, it's irrelevant unless that intelligence is communicated, consumed and actioned effectively. That has implications for the substance and conceptualisation of future intelligence products but also their format and means of delivery.

It's for this reason that the IIR found that:

> The business model for meeting the intelligence needs of executive government is no longer keeping up with demand and needs re-imagining so that a broader range of ministers can be supported more regularly, including in capitals other than Canberra.[155]

Just as the alignment between what staff can do in and out of the office with technology matters (see above), so, too, does the alignment between what consumers of intelligence can do with classified and non-classified information flows. Today's youthful consumers of information via video on demand, microblogging, apps of dizzying variety and AI interactions—and with dramatically altered attention spans as a result—will soon be the national-security policymakers and ministers of tomorrow. That will require significant innovation in future intelligence product from intelligence agencies.

As one informed commentator on intelligence matters made plain, 'Intelligence practitioners don't yet properly understand that the way human beings interact with knowledge is changing fundamentally.' It can no longer be assumed that 'intelligence customers are a "captive audience".' This should be sounding alarms for Australia's intelligence agencies because 'the NIC is less strategically relevant than it sees itself.'[156]

Other interviewees reflected self-critically on past efforts to innovate in this space, including clunky efforts to meet Malcolm Turnbull's particular information preferences when he ascended to the Prime Minister's office in 2015 (via stand-alone iPads configured for classified material).[157] Similar efforts were made to distribute cabinet documents over the 2010s, the limitations on which, according to one former official, 'rendered them no more useful, sometimes even less useful, than stacks of paper docs'.[158]

Typically, the default of Australian intelligence agencies has been back to product based on (albeit electronic) pieces of paper. As one former senior intelligence officer previously posted to Washington DC noted, the US system meets particular

customer requirements through having greater system access by policy officials and also 'through scale and people. They have policy staff (including military) on hand and ready to brief policymakers at a moment's notice.' Unable to deploy people at the same scale, but reluctant to embrace challenging technological options, 'We've tried to do it in Australia by having foreknowledge of [customers'] requirements, drivers.'[159]

This won't be enough to meet the oncoming challenge of distinct customer needs. Whether that's the expectation that future National Security Committee of Cabinet meetings 'on the fly' will become the norm rather than the exception,[160] or an acceleration of the trend towards 'less demand to simply know what is going on, and a greater focus on verification (maybe of information that is being speculated about) and on the "so what". Officials increasingly are asking what can be done about information; not just what it is …'[161]

It's for that reason that the IIR encouraged 'the development of innovative technological solutions to support the delivery of classified material to government more quickly and easily than is possible at the moment'.[162]

A particular future frontier will be the incorporation of AI into the process and product of all-source intelligence assessment—a topic canvassed by ASPI in 2024 jointly with the US Special Competitive Studies Project, the USIC and the NIC.[163] Future possibilities are already opening up, including the potential use of AI-driven interfaces for not only intelligence delivery but also intelligence requirements, mixed together in a single dialogue and challenging the very concept of what intelligence reporting is—or might be.[164]

Importantly, it's clear from the interviews undertaken that Australia's intelligence agencies are alive to the emerging requirement for innovation in intelligence production and are taking meaningful steps in that regard.[165] As one senior intelligence officer commented:

> On intelligence product, the bigger picture is the extraordinary pace of tech change. In my view, organisations do need to adapt and innovate to remain relevant and effectively meet requirements, while still being mindful of trade-offs.[166]

Recommendation 5: Intelligence agencies, led by ONI (and drawing on assistance from outside government), should expand on IIR recommendations in relation to future intelligence delivery to more generally prepare the NIC for future reinventions of intelligence product (such as the incorporation of AI into customer interfaces) to meet evolving customer needs and information-consumption preferences.

Avoiding 'innovation by workaround'

Contests involve both offence and defence. Just as the contest described above creates a strong imperative for innovation in Australia, the protective security considerations arising demand prudence and intentionality in adopting new practices in the national-security space.

That point is underlined by the US experience of 'Signal-gate', which was revealed only by the extraordinary mistake of including a journalist in the message thread. It appears that Trump administration cabinet officials widely used a commercial messaging app (Signal) to discuss sensitive—and arguably classified—national-security information.

That occurred despite the US national-security budget exceeding more than US$1 trillion—and despite the presumed availability of secure government-issued alternatives. Rather, Signal-gate demonstrates that, without purposeful innovation that incorporates security-mindedness across technological development and deployment (beyond just encryption), users will create vulnerabilities in the quest for convenience and the familiar functionality of personal options.

This isn't isolated to the US, even if the circumstances of Signal-gate seem particularly egregious, for the same impulses and somewhat similar behaviour are evident in the UK. A 2022 report by the Institute for Government revealed just how prevalent commercial messaging app use was in Westminster and Whitehall (in this instance, via WhatsApp). In addition to more general concerns about security, the report identified that WhatsApp's speed and accessibility had led to the accentuation of existing 'informal' government practices, resulting in the risk of 'poor decisions being made with incomplete information', more difficult record-keeping and scrutiny, and an undermining of 'accountability and transparency on official information'.[167]

Australians shouldn't feel superior in this regard. In February this year, the Australian Information Commissioner issued her own report on messaging app use within the Australian Government. That report found that 73% of responding agencies permitted the use of commercial messaging apps for government purposes, confirming 'that the use of messaging apps is an established feature of digital communication within government' but that such use 'is not well supported with policies and procedures'. Aside from concerns about record-keeping, including lawfulness, given the requirements of the *Archives Act 1983* (as amended), the report identified gaps in security policies. For example, only a quarter of agencies that permitted commercial messaging app use provided staff with policy advice addressing security classification per the Protective Security Policy Framework.[168]

The commissioner's report came on the heels of longstanding public concerns about the prudence and security of commercial app use across Australian governments, and an even longer global history of technical security issues as those apps have been developed and have evolved.[169,170]

The answer isn't to reject technology or innovations that enhance the speed and agility of government—particularly in national-security knowledge and decision-making—especially given the intensifying contest that Australia faces. Nor should we overlook how mobility can not only transform immediate communications but also enable far more agile and flexible ways of working across government.

The lesson, instead, is to embrace innovation that's both purposeful and secure from the outset—drawing on the UK's experience with secure mobility since the onset of the Covid-19 pandemic—particularly given the divergent imperatives and usage patterns between the UK and Australian governments.[171] This approach must combine robust technical security (including the most effective encryption) with a human-centered focus that recognises users as both the most significant security vulnerability and those best placed to assess and adapt to their security environments.

Relatedly, one former senior military officer familiar with secure mobility issues analogised in their interview that allowing ADF personnel to use personal electronic devices during the course of their work (and within the information domain) is like issuing a rifle: 'Do you use it anywhere, in any circumstance? No! You have practices, policies, instructions. And you hold people accountable for negligent discharges.'[172] That analogy works just as well for issuing national-security personnel with secure mobility devices!

Notes

1 Interview #20, April 2025.

2 Interview #23, May 2025.

3 The Australian Sovereign Capability Alliance (ASCA) provided a useful definition of the slippery concept of 'sovereign capability' in its submission to a 2021 parliamentary inquiry into Australian sovereign naval shipbuilding. According to ASCA: 'Sovereign capability concerns the industrial, economic, logistical, research and educational capabilities required by a country to achieve objectives including safety, defence, health and wellbeing, food security, energy and key materials supply, infrastructure security, and environmental sustainability. Sovereign capability addresses what we must be able to make and do, to achieve some level of self-sufficiency in areas where it matters most.' 'Submissions received by the committee', Senate Standing Committees on Economics, Inquiry into Australia's Sovereign Naval Shipbuilding Capability, Australian Parliament, online. See also Rajiv Shah, 'Sovereign capability can benefit Australia—up to a point', *The Strategist*, 17 April 2025, online.

4 This report is primarily based on responses given by interview participants. In the interests of candour (and noting some legislative constraints on the identification of individuals and on the publication of operationally sensitive information), anonymised descriptions have been used as a default when citing and quoting responses, although suitable context is provided as far as possible.

5 Interviewees were asked the following questions (only some of which were relevant to each interviewee):

1. How is 'contest' informing your thinking about capability and innovation (in general terms)? What is the related sense of 'urgency' (including in comparison with partners like the UK)?
2. Do you believe your organisation is well placed (in terms of capacity, opportunity etc.) to pursue innovation in national-security work practices?
3. Are there examples where technology has been successfully leveraged for work practice changes—and where it hasn't been successful? What were the broad themes of success and failure?
4. What organisational approach are you taking in relation to technology and your 'new' workforce (and their expectations)?
5. What approach are you taking to technology and the future of the intelligence interface (and product)?
6. Is there a 'sovereignty' dimension to your approach to technology, including in relation to traditional partners like the US?
7. The recent OAIC survey of Australian agency use of messaging apps and #Signalgate suggest that mobile communications workarounds are occurring across governments, despite security and governance risks. From your perspective, what are the biggest barriers to adopting secure mobile solutions that are fit for purpose?
8. Do you have related general observations on barriers to / constraints upon innovation in the national security space? What would aid your organisation in pursuing innovation? What, in your view, would aid others within the national-security community?

6 See also Michael Blanding, 'Failing well: how your "intelligent failure" unlocks your full potential', *Working Knowledge*, Harvard Business School, 5 September 2023, online.

7 Interview #6, April 2025.

8 Originally recommended in Chris Taylor, 'Intelligence and security: strengthening Australia's strategic advantage in a complex world', in *Agenda for Change: preparedness and resilience in an uncertain world*, ASPI, Canberra, April 2025, 44, online.

9 Interview #17, April 2024.

10 Matt Ridley, *How innovation works*, London, 2020, 4.

11 Follow-up comments from interview #2, as of May 2025.

12 ISO Standard 56000: 2025—'Innovation management: fundamentals & vocabulary', online. See also Diana Porumboiu, 'The ISO 56000 series for Innovation Management explained', *Hype Boards*, 26 July 2023, online.

13 Interview #3, April 2025.

14 Interview #16, April 2025.

15 Interview #28, May 2025.

16 Interview #11, April 2025

17 Interview #13, April 2025.

18 Interview #13, April 2025.

19 Interview #17, April 2025.

20 Interview #24, May 2025.

21 Signals intelligence (SIGINT): 'useful information gained from collecting, decrypting and analysing signals. Signals intelligence agencies collect and analyse information from the intercepted electronic communications of adversaries'. Australian Signals Directorate, online.

22 Department of the Prime Minister and Cabinet (PM&C), *2024 Independent Intelligence Review*, Australian Government, 2024, 23.

23 Interview #3, April 2025.

24 Interview #2, April 2025.

25 Interview #22, April 2025.

26 Interview #24, May 2025.

27 Interview #11, April 2025.

28 Interview #19, April 2025.

29 Interview #24, May 2025.

30 Interview #26, May 2025.
31 A gap highlighted in much of ASPI's recent work. See, for example, Raelene Lockhorst, Chris Taylor (eds), *Agenda for Change 2025: Preparedness and resilience in an uncertain world*, ASPI, Canberra, 29 April 2025, online; Marc Ablong (ed.), *The cost of Defence 2025: ASPI defence budget brief 2025–26*, ASPI, Canberra, 29 May 2025, online.
32 Interview #8, April 2025.
33 Interview #21, April 2025.
34 See Chris Taylor, 'Trump's upending of US intelligence: implications for Australia', *The Strategist*, 6 March 2025, online.
35 Interview #1, 8 April 2025.
36 Interview #2, April 2025.
37 Interview #28, May 2025.
38 Interview #6, April 2025.
39 Interview #7, April 2025.
40 Assisted by the categorisation of leadership, culture and risk found in *Maintaining the intelligence edge: reimagining and reinventing intelligence through innovation*, Center for Strategic & International Studies, January 2021.
41 Interview #6, April 2025.
42 Interview #16, April 2025.
43 Interview #10, April 2025.
44 Interview #4, April 2025; interview #25, May 2025.
45 Interview #4, April 2025.
46 Interview #22, April 2025.
47 Interview #24, May 2025.
48 Interview #20, April 2025.
49 Interview #20, April 2025.
50 Interview #28, May 2025.
51 Interview #3, April 2025.
52 Interview #20, April 2025.
53 Interview #3, April 2025.
54 Interview #17, April 2025.
55 Interview #20, April 2025.
56 Interview #20, April 2025.
57 Interview #25, May 2025.
58 Robert Hannigan, *Counter-intelligence: What the secret world can teach us about problem-solving and creativity*, London, 2024, 308.
59 Interviews #2 and #16, April 2025.
60 Interview #20, April 2025.
61 See, for example, Sara Howard, 'Thinking like a fox: the agile innovation mindset', *Australia Post*, 4 July 2017, online.
62 Follow-up comments from interview #2, as of May 2025.
63 'Cognitive diversity, leading change and intelligence policy with Carmen Medina', podcast with Miah Hammond-Errey (season 3, episode 4), *Technology and Security*, 15 April 2025. (As suggested in discussion of 6 May 2025.)
64 Interview #27, May 2025.
65 *Maintaining the intelligence edge: reimagining and reinventing intelligence through innovation*, Center for Strategic & International Studies, January 2021, 42.
66 Interview #4, April 2025; interview #10, April 2025.
67 Interview #13, April 2025.
68 Interviews #5 and #8, April 2025.
69 Interview #5, April 2025.
70 Interview #4, April 2025.
71 Interview #9, April 2025.
72 Interview #24, May 2025.
73 Interview #5, April 2025.
74 Interview #11, April 2025.
75 Interview #13, April 2025.
76 Miah Hammond-Errey, 'Is Australia's defence force, and the public service, too conservative?', *Canberra Times*, 2 October 2023.
77 Interview #19, April 2025.
78 Interview #24, May 2025.
79 Interview #13, April 2025.
80 Interview #11, April 2025.
81 Interview #3, April 2025.

82 Interview #5, April 2025.
83 Interview #5, April 2025.
84 Interviews #3 and #4, April 2025.
85 Interview #8, April 2025.
86 Interview #20, April 2025.
87 Interview #19, April 2025.
88 Interview #4, April 2025.
89 Interview #7, April 2025.
90 Interview #18, April 2025.
91 See, for example, Alex Osterwalder, 'The corporate innovation system', *Strategyzer*, 15 May 2025, online; Tandayi Viki et al., 'From innovation theatre to growth engine', *Strategyzer*, April 2023, online.
92 Interview #16, April 2025.
93 Interviews #13 and #17, April 2025.
94 Interview #19, April 2025.
95 Interview #5, April 2025.
96 Interview #13, April 2025.
97 Interview #19, April 2025.
98 Interview #18, April 2025.
99 Interview #15, April 2025.
100 Interview #26, May 2025.
101 Interview #24, May 2025.
102 Interviews #4 and #22, April 2025.
103 Interview #17, April 2025.
104 Interview #17, April 2025.
105 Interview #27, May 2025. See *2017 Independent Intelligence Review*, Australian Government, June 2017, 81, online.
106 Interview #16, April 2025.
107 Follow-up comments from interview #2, as of May 2025. See also Lucy Luo, 'The explore–exploit continuum', *Strategyzer*, 16 March 2020, online.
108 Interview #25, May 2025.
109 Interviews #23 and #26, May 2025.
110 Interview #18, April 2025.
111 See also Blanding, 'Failing well: how your "intelligent failure" unlocks your full potential'.
112 Interview #6, April 2025.
113 Australian Signals Directorate, 'REDSPICE—Resilience, Effects, Defence, Space, Intelligence, Cyber Enablers', Australian Government, no date, online.
114 See Ablong, *The cost of Defence 2025: ASPI defence budget brief 2025–26*.
115 Interview #28, May 2025.
116 Interview #25, May 2025.
117 Interview #4, April 2025.
118 See Chris Taylor, 'Intelligence and security: strengthening Australia's strategic advantage in a complex world' in Raelene Lockhorst, Chris Taylor (eds), *Agenda for Change 2025: preparedness and resilience in an uncertain world*, ASPI, Canberra, 42–43, 29 April 2025, online.
119 See, for example, Leonor Almeida, Antonio Moreira, 'Workplace innovation: a search for its determinants through a systematic literature review', *Business Theory and Practice*, 23(2):502–524; Peter Totterdill, 'What is workplace innovation?', European Workplace Innovation Network (EUWIN), no date.
120 Lucy Mason, Andrew Shortland, *National security innovation: creating new capabilities for the future*, Centre for Emerging Technology and Security, 21 September 2022.
121 Sebastiaan Rietjens, Rob Sinterniklaas, Stephen Coulthart, 'How intelligence organisations innovate', *Intelligence and National Security*, 2025, 40(1):24.
122 PM&C, *2024 Independent Intelligence Review*, 92.
123 Interview #5, April 2025.
124 See 'Millennials at work: reshaping the workplace', PWC, 2011, online; 'Generational research on technology and its impact in the workplace', CompTIA (Computing Technology Industry Association), June 2013, online; 'How to be an employer of choice for Gen Z: fulfilling the next-generation workplace wish list', Workforce Institute (Kronos Ltd), 2019, online; 'Gen Z—what are their career expectations?', McCrindle Research, 2020, online; 'Global Digital Employee Experience (DEX) Survey 2023', Riverbed Technology, online.
125 Interview #3, April 2025.
126 Interview #12, April 2025.
127 Interview #17, April 2025.
128 PM&C, *2024 Independent Intelligence Review*, 92.
129 Interview #4, April 2025.
130 John Kroger, 'Office life at the Pentagon is disconcertingly retrograde', *Wired*, 20 August 2020.

131 Interview #11, April 2025.
132 Interview #17, April 2025.
133 Interview #28, May 2025.
134 Interview #2, April 2025.
135 Interview #19, April 2025.
136 Interview #28, May 2025.
137 Interview #9, April 2025.
138 Interview #11, April 2025.
139 Interview #4, April 2025.
140 Interview #3, April 2025.
141 Interview #26, May 2025.
142 Interview #8, April 2025.
143 Interview #11, April 2025.
144 Interview #12, April 2025.
145 Interview #1, April 2025.
146 Interview #8, April 2025.
147 Interview #4, April 2025.
148 Interview #17, April 2025.
149 Interview #9, April 2025.
150 Interview #28, May 2025.
151 Interview #19, April 2025.
152 Interview #2, April 2025.
153 Interview #26, May 2025.
154 Originally recommended in Chris Taylor, 'Intelligence and security: strengthening Australia's strategic advantage in a complex world' in *Agenda for Change: preparedness and resilience in an uncertain world*, ASPI, Canberra, April 2025, 44.
155 PM&C, *2024 Independent Intelligence Review*, 8.
156 Interview #25, May 2025.
157 Interview #1, April 2025. See also Malcolm Turnbull's account in *A bigger picture*, Melbourne, 2020: 'Finally, I managed to persuade the intelligence agencies to share the reports on a secure iPad, which could be delivered to me wherever I was in Australia! That momentous reform aside …' (p. 436).
158 Interview #1, April 2025.
159 Interview #21, April 2025.
160 Interview #1, April 2025.
161 Interview #2, April 2025.
162 PM&C, *2024 Independent Intelligence Review*, 57.
163 Alexandra Caples, *The future of intelligence analysis: US–Australia project on AI and human machine teaming*, ASPI, Canberra, 3 September 2024, online.
164 Interview #25, May 2025.
165 Interview #24, May 2025.
166 Interview #18, April 2025.
167 Tim Durrant, Alice Lilly, Paeony Tingay, *WhatsApp in government: how ministers and officials should use messaging apps—and how they shouldn't*, Institute for Government, March 2022.
168 Office of the Australian Information Commissioner, *Messaging apps: a report on Australian Government agency practices and policies*, Australian Government, 27 February 2025; see also Elizabeth Tydd, Simon Froude, 'APS agencies need to sharpen their policies on messaging apps', *Canberra Times*, 19 March 2025.
169 For an Australian chronology, see David Stewart, 'Federal ministers love WhatsApp. But what does the law say about it?', *Information & Data Manager*, 21 October 2016; Bruce Baer Arnold, 'Banning MPs from private messaging apps is a simplistic response to a complex problem', *The Conversation*, 10 April 2018; Matthew Doran, 'Scott Morrison tries to switch focus to drought as WhatsApp messages reveal backroom bartering ahead of spill', *ABC News*, 26 August 2018; Moira Paterson, 'Yes, a WhatsApp message could be subject to FOI—but you'd have to find it first', *The Conversation*, 15 November 2018; Shane Wright, 'From pen and paper to Wickr: the battle to save government decisions', *Sydney Morning Herald*, 19 Apil 2021; Doug Dingwall, 'WhatsApp conversations with ministers, bureaucrats should be recorded: National Archives boss', *Canberra Times*, 15 April 2021 (via OAIC Estimates brief); Josh Taylor, 'Scott Morrison must reveal any text messages from Qanon friend, information watchdog orders', 31 March 2022, and 'Barnaby Joyce's drought envoy texts to Scott Morrison should be released, information watchdog rules', 2 April 2022, *The Guardian* (via OAIC Estimates brief); Stephanie Dalzell, 'Attorney-General warns politicians after confirming integrity commission could access encrypted texts on WhatsApp and Signal, *ABC News*, 2 October 2022; AAP, 'NSW police banned from using WhatsApp on work phones', *The Guardian*, 30 September 2024; Josh Taylor, 'Half of Australia's law enforcement agencies have banned officers using encrypted messaging apps', *The Guardian*, 12 October 2024; Josh Taylor, 'Australia's home affairs department has let staff use Signal since Covid lockdowns, documents show', *The Guardian*, 5 May 2025.
170 For a global perspective, see Jaikumar Vijayan, 'Security problems persist with instant messaging', *Computer World*, 9 May 2003; 'WhatsApp pursued for privacy violations', *Business Spectator*, 29 January 2013; 'Survey: 83 per cent of US organizations have accidentally exposed sensitive

data', *Businesswire*, 21 February 2019; 'WhatsApp security breach likely a government surveillance attack, company says', *ABC News*, 15 May 2019; 'WhatsApp users targeted by spyware via in-app phone call prompting upgrade calls', *ABC News*, 15 May 2019. See also 'WhatsApp major security flaw could let hackers access phones', *CNN*, 15 May 2019; *Forensic methodology report: how to catch NSO Group's Pegasus*, Amnesty International, 2021; Andy Greenberg, 'How Safari and iMessage have made iPhones less secure', *Wired*, 9 September 2019; Lily May Newman, 'Apples fixes one of the iPhone's most pressing security risks', *Wired*, 30 January 2021; although also see Ben Gilbert, 'Apple's iPhone has a "major blinking red five-alarm-fire problem with iMessage security," according to a cybersecurity researcher', *Business Insider*, 20 July 2021 (linked to Amnesty International investigation); 'Twilio incident: what Signal users need to know', *Signal Support*, July 2022; Graham Cluley, 'Signal debunks online rumours of zero-day security vulnerability', *Bitdefender*, 17 October 2023; Chiara Castro, 'Signal rejects "dangerously misleading" security flaw allegations', *Techradar*, 2 December 2023; Zak Doffman, 'New report exposes security issues with WhatsApp apps', *Forbes*, 7 July 2024; Zak Doffman, 'FBI warning—you should stop using iMessage on your iPhone, *Forbes*, 15 December 2024; Bill Chappell, 'FBI warns Americans to keep their text messages secure: what to know', *NPR*, 17 December 2024; 'CISA urges switch to Signal-like encrypted messaging apps after telecom hacks', Cybersecurity and Infrastructure Security Agency, US Government, 18 December 2024; Lawrence Abrams, 'Phishing texts trick Apple iMessage users into disabling protection', *Bleeping Computer*, 12 January 2025; Bill Goodwin, 'Warning over privacy of encrypted messages as Russia targets Signal Messenger', *Computer Weekly*, 19 February 2025; Ryan Naraine, 'How Russian hackers are exploiting Signal "linked devices" feature for real-time spying', *Security Week*, 19 February 2025.

171 Interview #14, April 2025.

172 Interview #8, April 2025.

Acronyms and abbreviations

ADF	Australian Defence Force
AI	artificial intelligence
CIA	Central Intelligence Agency
CSIRO	Commonwealth Scientific and Industrial Research Organisation
IIR	Independent Intelligence Review
NIC	national intelligence community
ONI	Office of National Intelligence
SMEs	small and medium-sized enterprises
STEM	science, technology, engineering and mathematics
TSOC	transnational serious organised crime
USIC	United States intelligence community

ASPI
AUSTRALIAN
STRATEGIC
POLICY
INSTITUTE

ISSN 2200-6648