SPECIAL REPORT

Collaborative and agile

Intelligence community collaboration insights from the United Kingdom and the United States

Michael Shoebridge,
Dr John Coyne and Dr Rajiv Shah

November 2021

ASPI
AUSTRALIAN STRATEGIC POLICY INSTITUTE

TWENTY YEARS OF ASPI STRATEGY
2001 - 2021

ASPI

About the authors

Michael Shoebridge is Director of Defence, Strategy and National Security at the Australian Strategic Policy Institute (ASPI).

Dr John Coyne is the Head of the Northern Australia Strategic Policy Centre and head of the Strategic Policing and Law Enforcement program at ASPI.

Dr Rajiv Shah is a Fellow with the International Cyber Policy Centre at ASPI.

Acknowledgement

ASPI would like to acknowledge BAE Systems' 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.

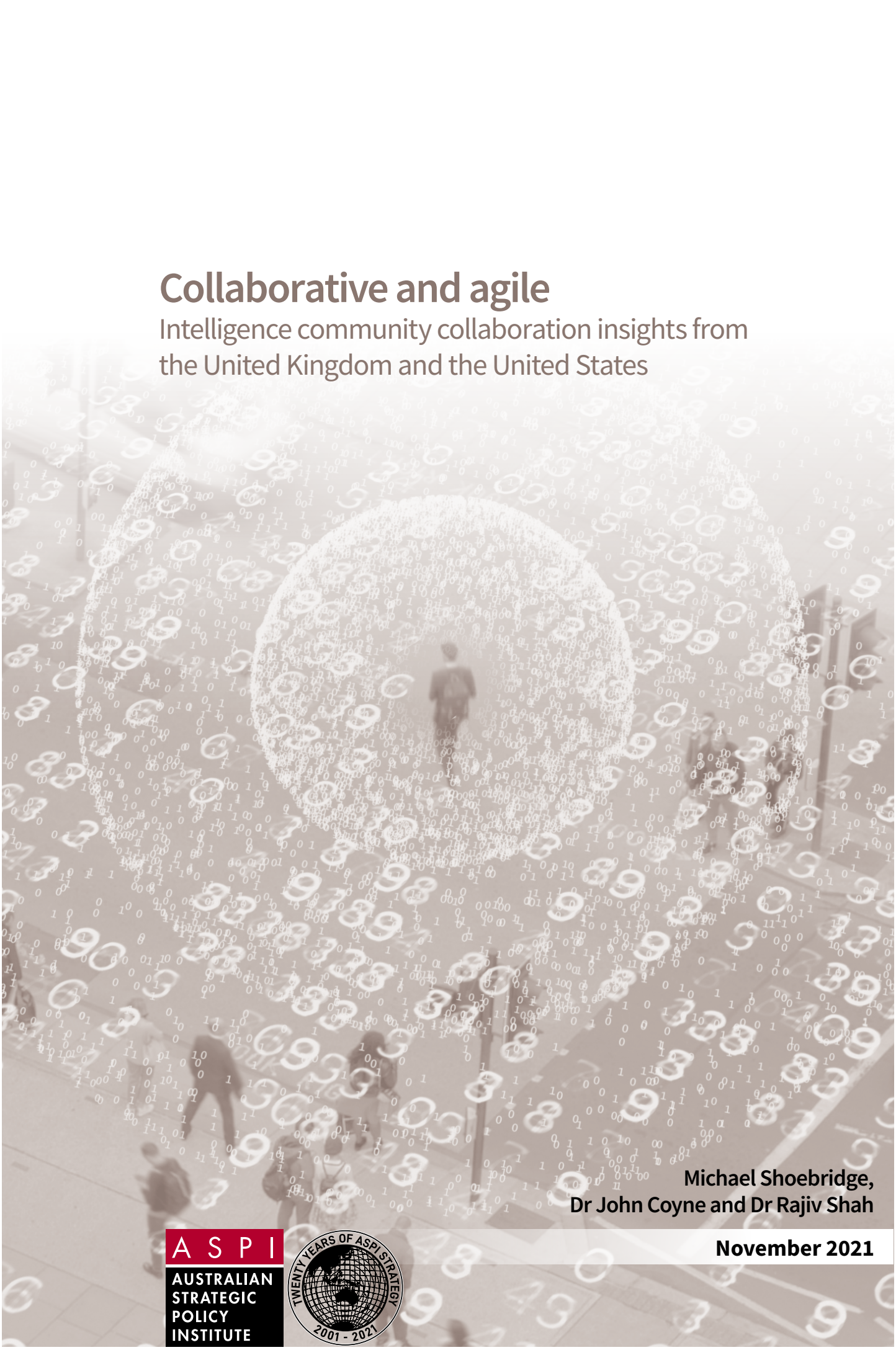
ASPI's publications—including this paper—are not intended in any way to express or reflect the views of the Australian Government. The opinions and recommendations in this paper are published by ASPI to promote public debate and understanding of strategic and defence issues. They reflect the personal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

Funding support for this publication was provided by BAE Systems.

Cover image: Visualisation of a radio signal coming from a mobile phone in a data filled scene, iStockphoto, peterhowell.

Collaborative and agile

Intelligence community collaboration insights from the United Kingdom and the United States



Michael Shoebridge,
Dr John Coyne and Dr Rajiv Shah

November 2021

ASPI
AUSTRALIAN STRATEGIC POLICY INSTITUTE

TWENTY YEARS OF ASPI STRATEGY
2001 - 2021

First published November 2021

Published in Australia by the Australian Strategic Policy Institute

ASPI
Level 2
40 Macquarie Street
Barton ACT 2600
Australia

Tel + 61 2 6270 5100
Fax + 61 2 6273 9566
Email enquiries@aspi.org.au
www.aspi.org.au
www.aspistrategist.org.au

Facebook.com/ASPI.org

@ASPI_org

Contents

Executive summary

At the time of the Independent Intelligence Review in 2017, extremism, state and non-state actors, climate change and technological change were all parts of the operating environment, along with rising competition between states. Covid was in our future. The digital world was providing a challenge to intelligence communities through the pace of technological change and the volumes of data available outside the classified world.

In 2021, this data and tech explosion is accelerating, and the challenge from it remains.

But the digital challenge to intelligence agencies varies from mission to mission. Some missions, such as counterterrorism, have a broad global footprint and common data-collection and analytical challenges despite the disparate human terrain and the historical and geographical dynamics that shape the counterterrorism environment differently in the Middle East, across the Indo-Pacific, and in Europe, North America and Australia.

It's clear now, though, that for Australia's intelligence community, success or failure in the broad China mission will be the primary performance test for successive governments over the next five and ten years. Even if the recent AUKUS partnership is focused on defence, not intelligence, it just reinforces this judgement about where national priorities have moved to since 2017 because of the shifts by China under Xi Jinping.

The combined challenges of the China mission arise out of the nature of the Chinese state, its domestic controls and its technological development. In some ways, China's burgeoning digitisation creates multiple digital vulnerabilities, including from its patchwork of party-state organisations and provincial and central government initiatives and systems, with all the system and human frailties and vulnerabilities that create seams for intelligence exploitation and access.

Some vulnerabilities also flow from Xi Jinping reasserting the centrality of Chinese Communist Party (CCP) and peak leader control, which includes the aggregation of national data for central government use. The CCP's attempts to strengthen control of itself (and its 90 million plus party members) and of the Chinese corporate and social worlds through technology bring all the digital vulnerabilities being experienced in other parts of the world, potentially to a greater degree.

Add to that the bifurcation of high technology and digital systems between China, its 'technology customer base' in major parts of the Indo-Pacific and Africa and the alternative technology bases of the G7, Quadrilateral Security Dialogue and AUKUS economies.

Some good news comes from the fact that the UK and US intelligence communities that this study examines largely share this urgency and priority, while retaining other pressures and priorities in each case (Russia and 'the globe', respectively).

Against all of this, the outbreak of Covid-19 has increased the speed and intensity of change and has broken or at least reshaped some approaches that once seemed settled and unquestionable. This brings with it opportunity.

Many nations—and their populations—have lost faith in simple market forces and assurances from corporate providers about the resilience and redundancies built into commercial arrangements, bringing about a new focus on resilience and sovereignty. Along with the effect of a coercive China, this is likely to cause an even more significant global economic and security dispersion away from the previous era of simple globalisation. That's a shift to how data and information will move in the world.

In many societies, including our own, users are becoming more security and privacy conscious; however, a significant portion of the growing 'open-source' data that users are creating is readily available, although harvesting and processing it within the ethical and legal framework of a democracy requires great effort. Even if someone is trying to minimise their digital footprint, it's increasingly difficult to function in society without leaving a trail of potentially discoverable data—a digital snail trail.

Given all this, it seems clear that incremental change to how things are done now isn't the path to success. So, what's to be done?

Our UK and US partners show us that an urgent mission focus creates the conditions for success in a way that top-down structural reforms or budget efficiency measures just don't.

The China mission is that 'burning platform' for change and success for Australian agencies, particularly those with a foreign intelligence focus such as the Australian Signals Directorate, the Australian Secret Intelligence Service, the Defence Intelligence Organisation and the assessment element of the Office of National Intelligence (ONI). But the China mission must include the Australian Security Intelligence Organisation in the area of foreign interference and counter-espionage. It's a team sport in the mission focus, technology, tradecraft and data senses.

Arguably, this grouping of agencies is the 'minilateral' within the larger national intelligence community that must combine most closely and urgently on the China mission. This reverses the 'all one community' concept of the broadened national intelligence community that was proposed in 2017. It also requires some unpicking of the 'return of the portfolio' in the intelligence community—which has manifested itself in the rise of the Department of Home Affairs as a director of its portfolio agencies, and to a lesser extent in the Defence organisation with the emergence of a new Chief of Defence Intelligence and the Defence intelligence Enterprise. That'll involve hard yards in the bureaucratic realms of Canberra.

The distinct attributes of the China mission require a distinctive approach as the high-technology decoupling between China, Australia, the US and other powerful democracies deepens. Decoupling, at least in the high-technology sector, is an 'unthinkable' that just keeps happening.

Lessons from dealing with denied areas during the Cold War era are relevant. However, the scale of data on mainland China available from non-intelligence means, such as commercial satellite imagery, combined with the continuing strengths of human intelligence and the inherent vulnerabilities in China's multilayered, complex digital systems working through the equally complex, unstable institutional party-state structures, provides the seeds for mission success.

Our US and UK partners also show us that unexpected crises such as Covid-19 can make unthinkable changes necessary and achievable: UK agencies' successes in developing applications and tools on the unclassified 'low side' over the past 18 months are an example.

Another lesson is the powerful capability lift and more rapid problem solving that can come from deeply engaged, trusted corporate partners who bring skills, concepts and technologies—which won't happen in our intelligence community unless traditional procurement models are challenged and changed.

In the UK environment, each agency still has its own requirements for bespoke technical capabilities for its particular remit and operating environment. However, standardised design principles and identifying which components of technology are reusable have helped to drive efficiency and cost savings and make agencies' capabilities interoperable.

And running faster acquisition is possible without completely reinventing federal government procurement—as proven by the ONI's Delivering Innovation through Procurement award in 2020. UK and US approaches for more urgent and more imaginative capability development, such as the UK's Cyber Accelerator and its British Business Bank-operated National Security Strategic Investment Fund, and the US's In-Q-Tel and Intelligence Advanced Research Projects Activity (the US intelligence community's equivalent to the Defense Advanced Research Projects Agency), all seem worth either partnering with or modelling.

Tradecraft in intelligence collection and analysis must now change to exploit open data sources, and not just have 'open-source' centres running in parallel to traditional classified tradecraft and collection activities. And analysis must move away from more traditional inductive analysis.

Artificial intelligence and machine-learning approaches, along with techniques such as data visualisation and data fusion to empower analysts, require novel technical specialists. Those people will stay only if the agency and government leaders and decision-makers are open to at times confronting, uncomfortable advice and have enough confidence to trust the advice of what, on occasions, can be staff in relatively junior or obscure roles. Recruiting and retaining such specialists will depend on them seeing the impact of their work. Trusted corporate partners—big and small—are part of winning this war for talent.

More collaborative and agile strategic intelligence involves finding new ways to bring classified data together with open-source bulk data. While this has been at the heart of the US intelligence community's pursuit of reform, its experience shows that this is a long and challenging process. In the Australian context, this must first overcome the national intelligence community's strong tribal cultures, which are so often resistant to change, along with the natural pride of intelligence professionals steeped in existing tradecraft. This is the 'industrial relations' aspect of change for intelligence.

The prioritisation of open sources doesn't mean an end to specialist covert data collection. Rather, it creates an enhanced opportunity for combining secret and open-source data to develop new insights.

Lastly, we see here and in our two big partners that leadership matters. The two key leadership challenges for Australia's intelligence community are to recognise the priority and distinct nature of the China mission, and to understand that individual agency (and intelligence community) success requires behaviours to shift to delivering insights from more common technology platforms and the exploitation of shared data, albeit leavened by agency-specific applications and (limited) bespoke data.

Future intelligence successes will be the rewards for intelligence communities that have the best datasets; can leverage the combined value of both secret and open sources; exploit those datasets, collection capabilities and analytical processes fastest; understand the distinct nature of key missions; and are open to the adoption of unfamiliar technologies and approaches from the world outside intelligence before such approaches proliferate to the level of obviousness.

This is an extraordinarily rich if difficult time to be in the intelligence community, whether in Australia or in our key allies and partners.

Introduction

In recognition of the changing strategic environment, and the increasing complexity of the intelligence mission across government, Australia's 2017 Independent Intelligence Review acknowledged the success of individual agencies but quickly added:

> A central theme of this report is to provide a pathway to take those areas of individual agency excellence to an even higher level of collective performance through strengthening integration across Australia's national intelligence enterprise. The aim is to turn highly capable agencies into a world-class intelligence community.[1]

The review's recommendations set in motion several structural changes to Australia's national intelligence enterprise.[2]

Since 2017, the old Australian intelligence community's membership has broadened with the addition of several new members.[3] The new members have come with a new national security community construct, resulting in further minor adjustments to our national intelligence enterprise. If anything, this broadening of the community, bringing in an even more diverse set of agencies, has brought about greater coordination, but it has brought to the surface the existing tribal nature of our Australian intelligence agencies. Regardless of the goodwill of many involved, an often intense sense of tribalism has prevailed, often manifested in passive resistance to change, especially with respect to interagency cooperation.[4] Several other themes across government and agencies have reinforced the centrality of agencies over the community construct. Within this, agency heads are the defining decision-makers for their agencies' particular interests.

The recommendations of the 2020 *Comprehensive Review of the Legal Framework of the National Intelligence Community* did even less to promote transformative change.[5] Instead, it did little more than advocate for adjustments at the fringes. Those and subsequent changes have often not been able to deal with the underlying cultural, organisational and policy challenges that have prevented enhanced intelligence collaboration.[6]

The scale of the US intelligence community means that there are insights available from it that demonstrate both paths not to take and pitfalls to avoid, as well as good practice to be thought through as it applies in Australia's own, different, smaller intelligence community operating within our economy and system of government. In contrast, the UK intelligence agencies provide insights closer to our own challenges—in that case, the scale and breadth are similar to Australia's intelligence community, but there are differences in industry partnerships and in the experience of change over the past two decades. In the past 18 months, there have also been some very practical approaches to the development of applications and the use of commercially derived tools in the UK, driven at least in part by the imposed constraints of working remotely from normal sites.

Both these Australian partners are dealing with the same core challenges Australian agencies face: a growing number of high-priority issues that policy- and decision-makers require insights about, an increasing competition for resources to cover the range of issues in a meaningful way, and a 'relevance challenge' to add insights that matter in an increasingly dense and rapid information flow that decision-makers are exposed to.

There's a more immediate and more political challenge that flows from events in 2021, too. Whatever the inside story about intelligence analysis and advice, the unexpectedly rapid fall of the Afghan Government and dissolution of the Afghan National Security Forces, combined with public statements from political and military leaders about that being unlikely in the months and weeks leading up to those events, no doubt raise questions in Washington and London about the effectiveness and insights that intelligence agencies produce—as well as their impact on decision-makers' understanding and directions. That pressure can be a useful catalyst within those intelligence communities to shift business models, challenge tradecraft in the light of the different digital world in which intelligence now operates, and take some larger steps than those contemplated in recent reviews.

Afghanistan has offered the US intelligence community a warning light that may in time become a tipping point for further structural change. For Australia's intelligence community, the withdrawal of the ADF and closure of our embassy before the fall of Kabul and the smaller scale of Australian involvement mean that it's unlikely to be a primary factor driving change here.

While the Australian debate on the future of our national intelligence enterprise remains largely behind closed doors, it's almost certainly fixed firmly on addressing the problem of a dynamically growing and evolving intelligence challenge: China. This is a systemic challenge that our UK and US partners are facing with us, noting our differing national interests and objectives.

Rapidly rising and increasingly assertive China has brought about a scale of global change—and challenge—not represented within the 2017 Independent Intelligence Review. In contrast to the review's all-hazards approach, today's China intelligence mission is complicated by the scale, depth and breadth of the threat to international systems and to the regional and global order that crosses strategic, technological, economic and environmental domains from a state actor that can direct all its national entities, public and private, towards its priorities. That state has enormous internal challenges, contradictions and tensions. It's also pressuring others and working to repurpose international institutions and rules to orbit around its interests and perspectives, in the Indo-Pacific and globally.

At the time of the Independent Intelligence Review in 2017, the digital world was providing a challenge to intelligence communities through the pace of technological change and the volumes of data available outside the classified world. In 2021, this data and tech explosion is accelerating, and the challenge remains.

But the new driving feature that must shape Australia's intelligence community is the increasing priority of 'the China mission', together with the difficulty of access and insight for that mission.

As with any authoritarian state, insights into Chinese state and Chinese Communist Party (CCP) deliberations and decision-making dynamics are always difficult. But access to data and insights into broader dynamics within China are being complicated by the nature of Xi Jinping's rule, which is more closed to diverse voices and inputs than previous regimes since Mao. It's also complicated by Chinese authorities' efforts to make China a harder digital target as part of the recentring of China on the CCP's authority and greater control of mainland data. This isn't all a positive agenda for Beijing, however, as it's occurring partly owing to the Chinese authorities' continued anxiety about the combination of the influence that external information can have on the Chinese population and to the inherent vulnerabilities of China's information environment that flow from China's deepening digitisation and complicated government and party structures.

The trend towards economic decoupling between China, the US and the broader 'West' makes the China data issue unique and distinct from the general challenge that digitisation and technological change provide to Australia's intelligence community. This is particularly because the focus of that nearer term 'decoupling' is in the high-technology sector. And Chinese technologies and companies diffusing internationally bring data collection, control and access by Chinese authorities—through companies and government agencies—beyond the borders of mainland China, enabled by the extraterritorial ambition and reach of the Chinese party-state despite international law and norms.

How Australia's intelligence community approaches this China mission is the single defining issue for at least the next decade. Success or failure in this broad mission is likely to be the primary performance test for the intelligence community under successive governments over that period. Some good news comes from the fact that the UK and US intelligence communities that this study examines largely share this urgency and priority for the China mission, along with some other pressures and priorities in each case.

It seems clear that incremental change to how things are done now isn't the path to success, given this environment. A slow evolutionary approach to the development of the national security community could well be accepted if not for the broadening scope and complexity of the national intelligence mission and the defining priority of the China mission.[7] The breadth of national security threats keeps on expanding. In parallel, strategic risk continues to grow—up to and including a credible risk of major-power war in coming years.[8]

Given the rapidly growing volumes of unclassified data (together with increasing collections of classified data as technologies and platforms come into service), agencies need to enhance their capacity not just to ingest but to analyse and generate insights from that stream.[9] At the same time, as they deal with the volume and velocity of open-source data, analytical and collection agencies alike need to leverage secret intelligence collection better.[10]

Technology development cycles have also accelerated—much more obviously in the speed of adoption and development in the corporate world than in the government world, including across Australia's Five Eyes partners. Bleeding-edge analytical capabilities are now available to state and non-state actors alike, and at speed. And some now widely used and accepted technologies and approaches in the commercial world, such as cloud computing, artificial intelligence and data analytics, are still underapplied in our intelligence community.

The gap between valuable approaches and technologies used elsewhere and the capabilities of our intelligence community seems likely to widen in this decade without change both to how the community operates and works together and to the business processes it uses to develop and acquire capabilities. There are clearly workforce and skills issues involved here, too. One path for addressing some of those issues is partnerships with trusted corporate entities who understand the constraints, contributions and powers of intelligence agencies within democracies. Traditional government acquisition models and policy cycles aren't always supporting agencies in closing their technology lag.[11]

At the same time, other state and non-state actors can adopt new technology rapidly. And agencies can do more than simply recognise and at times rail against larger government procurement rules and processes, and instead propose alternative models that work at the speed that the environment of intelligence requires.

Australia's national security community has served the country well; however, change must occur to ensure that it remains ready to support the nation into the future. It has deep relationships, agency-to-agency partnerships and histories with the UK, the US and other close partners, notably in its Five Eyes counterparts. With that network of relationships and partnerships, our intelligence agencies have many opportunities to identify innovations that have promoted collaboration and agility within their respective intelligence communities.

This report explores critical policy, cultural and technological collaboration insights from the US and UK efforts to bring together their intelligence communities. The report pays particular attention to the work undertaken in the UK to break down the tribal silos between the various agencies within the community: military or civilian, collection or analytical, internally or internationally focused. The report considers insights into how intelligence communities can achieve technological advantages through a collaborative and agile approach.

Aim

The primary research question underpinning this body of work is:

> What insights from the UK and US intelligence communities can the Office of National Intelligence (ONI) use to promote greater collaboration and agility in Australia's national security community?

The central aim of this applied policy research project is to generate insights from the US and UK intelligence communities' collaboration efforts. This report identifies insights so that members of Australia's national intelligence community, including the ONI, can use them to enhance the community's collaboration and agility for the purpose of giving Australian decision-makers an insight edge over others. We acknowledge that agencies must contextualise those insights to Australia's specific circumstances, and we've sought to do some of that in this report. The report isn't intended as an academic think piece but as a guide—and goad—to actions that can advance and protect Australia's wellbeing, prosperity and security.

Methodology

This research used explorative qualitative methods. The research team used comparative case studies of the US and UK experiences in promoting and nurturing intelligence-community collaboration and agility. Data was collected using a variety of primary sources from both the public and the private sectors. The research team used semi-structured interviews with individuals and small groups to collect data.

This report doesn't seek to second-guess the internal insights that it explores. Instead, it takes an external perspective, informed by experience in relevant agencies and by perspectives from intelligence-community partners and analysts in the UK and the US.

That this is an unclassified exercise is an advantage when it comes to communicating the findings. However, that also imposes limitations on the collected data and its analysis.

The strategic context

In their report of the 2017 Independent Intelligence Review, Michael L'Estrange and Stephen Merchant went to some length to explore Australia's national security environment of the day and the changing contours of the national security outlook.[12] The review focused on preparing Australia's intelligence enterprise for future demands and expectations in the nation's changing international security context. Understandably, with that forward focus, the assessment of the strategic context was far more forward-leaning and pessimistic about the increasing strategic uncertainty that Australia would face than the *2016 Defence White Paper*.[13]

L'Estrange and Merchant painted a picture of powerful, rapidly evolving forces of change that reshaped the very concepts of security. The review argued that those forces were recalibrating how nation-states and people interact.

The review posited that three focal points drive the pace and intensity of change to the Australian intelligence community's strategic context: changes to the international system, extremism with global reach and the impacts of accelerating technological change.

The review also highlighted the destabilising impacts of the enhanced asymmetrical capabilities of non-states. In the four years that have passed since then, the asymmetric influence of particular non-state actors has shifted and may shift again. Islamist terrorists are obvious examples, although the rise in reach and power of non-state technology definers and users has become more pronounced, as has the intrusive reach of Beijing's authoritarian state enabled by its own technology firms and non-state helpers. However, overall, the review's assessments of Australia's national security environment were accurate, at least in the overarching analysis, although, arguably, the review's assessments, like those in the *2016 Defence White Paper*, appear somewhat optimistic with the benefit of hindsight, notably on the tempo of change and its implications.[14]

The rapid rebalancing of power and wealth, the interaction of economic globalisation and geopolitical power politics, and technological changes have all influenced Australia's security environment. However, the velocity and scale of the changes have already outpaced those anticipated in the review.[15] That change has been aided in no small part by the arrival of Covid-19,[16] accelerated asymmetric grey-zone activity,[17] an unprecedentedly more assertive China,[18] and still-accelerating technological change.

So, where does that leave us today? And what will Australia's future national security environment look like?

Of course, when L'Estrange and Merchant wrote their review report, convention demanded that they speak to the general national-security environment, so they were understandably careful not to highlight specific challenges in order to avoid diplomatic repercussions, media hype and public panic. If we were to follow similar conventions, it would be sufficient to say that the security environment is, and will continue to be, dominated by accelerating uncertainty and unpredictability in many areas. But that would be deeply unhelpful and, given the obvious overt challenges in our world, superficial. With more granularity, there's a growing certainty about the challenge that China poses systemically to Australia and other open societies. The deepening of the resulting competition between China and the world's powerful democracies (notably, but not just, the US) brings at least high-technology decoupling, along with expanded asymmetric conflict and influence operations. However, such broad descriptions don't have sufficient granularity to allow us to consider the future of intelligence as an enterprise, process or product.

By 2017, the Australian intelligence community warmly welcomed the end of the all-hazards approach to national security introduced under the Rudd government.[19] As traditionalists, L'Estrange and Merchant probably felt some comfort that the scope of national security had returned to a focus on the international security environment. A closer analysis of the review reveals that the authors had indeed sought to make the review more radical, with a focus beyond traditional national security. Without the benefits of hindsight, the reviewers couldn't foresee the speed and scale at which our strategic certainty would degrade (they were in plenty of good company on that), nor how accelerated broader technological and social changes would see once-in-a-decade intelligence challenges arrive every 18 months, with no sign that this phenomenon will stay the same, let alone slow.

Today, while we're a long way from the often confusing all-hazards era, the traditional scope of national security has changed forever. The all too familiar conceptual 'red lines' and 'silos'—including institutional and organisational ones—are increasingly unhelpful constructs. The line between national and domestic security is a case in point. Binary international and national perspectives on terrorism, crime, foreign influence and social cohesion are no longer helpful, if they ever were. The red lines between economics and national security and state and territory and federal policy loom large.

Those blurring demarcation lines are illustrated in no small part by the Australian Government's ending of the agreement between the Victorian state government and the CCP on the Belt and Road Initiative because it was inconsistent with Australian foreign policy interests.[20] The blurring is also demonstrated by the federal government's decision to exclude certain vendors from providing 5G technology, which a few years ago would have been decided through a predominantly economic lens but has instead been a clear case of needing to integrate economic, technological and national security issues into government decision-making.

So, the scope changes for the intelligence community can no longer be adequately defined by traditional parameters; for example, by describing them as strictly domestic or foreign intelligence missions. The scope is now characterised by four big drivers—Covid, climate change, China and technology—but unfortunately it isn't simply reducible to just those drivers. Some enduring threats and pressures remain and react with them—violent extremism being one (Figure 1).

Figure 1: Taliban occupy the Afghanistan Presidential Palace

Source: Flickr/Daniel Moskowitz, online.

Non-state actors continue to have broad global impacts. The 'Global War on Terror' lumbers towards the start of its third decade with little to suggest that the threat from Islamist terrorism is reducing, but showing a clear pattern of dispersal and diffusion of actors and groups beyond the simpler categories of the past 20 years. And old focuses remain relevant, albeit changed.

The return of the Taliban in Afghanistan, this time in a more media-savvy guise with a more articulate pitch to various possible international benefactors is an example, along with continued conflict in Syria and Iraq and the actions of various terrorist groups in our near region, inspired by local dynamics but with international connections.

And, as Mike Burgess, the Director-General of the Australian Security Intelligence Organisation (ASIO), has observed, there are terrorist threats beyond the familiar Islamist extremist sources, including the prospect of right-wing extremists turning to violence to achieve their goals (Figure 2). Like Islamist extremism, resurgent right-wing extremism encompassing beliefs ranging from white supremacy to violent ultranationalism is finding a broader global audience through social media.[21]

Figure 2: Proud Boys at the second million MAGA march in Washington, DC in December, 2020

Source: Flickr/Geoff Livingston, online.

In short, the Islamist-inspired terror threat of today is very different from the one that was highlighted in the 2017 intelligence review. Despite that change, the political dimension of the problem, including zero tolerance for intelligence failure, make adaptation and rebounding to reallocate efforts towards the China mission difficult.

Rogue states such as Iran and North Korea continue to acquire technology and, in doing so, are rapidly developing new offensive strike and asymmetric capabilities (Figure 3).[22] In acquiring and operationalising those capabilities, rogue states are leveraging the increasing complexities of the broader international security context to obfuscate their activities. The combined impact of their often erratic strategic calculus and a more broadly focused international security community is creating opportunities for them to use strategic surprise.

Figure 3: North Korean missiles

Source: iStockphoto/narvikk, online.

A resurgent Russia under President Vladimir Putin, despite its worsening demographic and economic troubles, continues its grey-zone activity in the Middle East, Ukraine and beyond (Figure 4). It's creating more significant strategic uncertainty across Europe, as well as stoking dissent and grievance in the US, as demonstrated in the 2016 and also the 2020 US presidential election campaigns.[23] While it's a long way from Australia, Russia distracts Australian allies and partners from considering the broader bifurcation of the international order by a more assertive CCP and raises the dangerous prospect of an increasingly close China–Russia partnership, despite enduring mutual suspicion. The Kremlin also remains a wild card in the Indo-Pacific.

Figure 4: Vladimir Putin, President of the Russian Federation, addresses the general debate of the General Assembly's seventieth session

Source: Flickr/United Nations photo, online.

The systemic challenge of China, faced by numerous powerful states and emerging out of the simpler dynamic of great-power competition between the US and China, further increases the velocity and scope of change to the contours of Australia's international security context. The Indo-Pacific and Australia are key political, military, technological and economic terrain for the systemic challenge from Xi Jinping's China to open societies globally. The CCP is assertively challenging the rules-based order across multiple fronts, from economic coercion, military build-up, wolf-warrior diplomacy, assertive maritime strategies and foreign interference to numerous border disputes. It uses its broad engagement and international representation and influence operations to treat its issues with other states as bilateral ones, rather than acknowledging the parallels in multiple relationships between China and others, in order to obscure the implications of its larger strategy. However, the CCP's tactical approach to managing international affairs is showing diminishing returns, as seen in the increasingly convergent assessments on China in the major economies of the democratic world and in the Indo-Pacific.

The increasing speed of technological life cycles is also ensuring rapid social, economic and security change.

Against all of this, the outbreak of Covid-19 has increased the speed and intensity of change and has broken or at least reshaped some approaches that once seemed settled and unquestionable. The pandemic has disrupted overall economic globalisation by disrupting particular supply chains and sectors (personal protective equipment and pharmaceuticals, but also the global automobile and semiconductor industries). Beyond those more obvious effects is the perhaps more important exposure of fragilities and single points of failure in what many assumed were

resilient corporate arrangements that would manage disruptions in a smoother and more effective way than we've seen. Many nations—and their populations—have lost faith in simple market forces and assurances from corporate providers about the resilience and redundancies built into commercial arrangements, bringing about a new focus on resilience and sovereignty.

This, when combined with the coercive way the Chinese state controls its people and access to its economy, seems likely to drive even more significant global economic and security dispersion away from the previous era of globalisation. It seems to also be shifting supply-chain models from the previously overarching trend towards inventory optimisation through just-in-time supply and a relentless focus on lowest cost supply options—almost regardless of geography and jurisdiction—in favour of a greater focus on performance and resilience from now expected natural and state-driven disruptions.

These rapid economic, social and geopolitical changes disrupt the plans of both great powers and introduce new areas where governments will seek the advantages available from intelligence insights.

Technology is changing the world, but decoupling brings defining differences …

The information and technology environment has changed dramatically over recent years. Computational power has continued to grow exponentially, in line with Moore's Law, and in defiance of the pundits who held that we were reaching fundamental limits a decade ago. This has been combined with the miniaturisation and portability of computing devices, such that most of us today carry devices in our pockets with more computational power than the supercomputers of yesteryear that filled entire buildings.

We've also seen the advent of ubiquitous, cheap, mobile communications—just in time to power the dislocated remote working we've had to do during the Covid pandemic. Massive increases in the data carrying capacity of fixed lines, the rollout of ever faster mobile networks and the now commonplace public Wi-Fi networks that are free at the point of use mean that it's the exception rather than the rule when that device in our pocket cannot wirelessly send and receive data at high speeds, and at a marginal cost per communication that's either zero or negligible.

Those changes, along with changes in societal attitudes which make people comfortable with communicating significant amounts of information with others, have enabled an explosion in data that's stored in computers and data centres and sent across telecommunications systems. The explosion hasn't been only in the volume of data, but also in the variety (consider the number of apps on a typical smartphone) and the velocity of technological change, as new apps come to prominence and others go out of fashion.

While users are becoming more security and privacy conscious, a significant portion of that data is readily available, although harvesting and processing it requires great effort. Even if someone is trying to minimise their digital footprint, it's increasingly difficult to function in society without leaving a trail of potentially discoverable data—a digital snail trail. Even with the increasing use of end-to-end encryption for the content of one-to-one communications, there's still a potential treasure trove of metadata from such communications, as well as from public and group communications that aren't encrypted.

As well as truly 'open-source' information, a wide range of commercial datasets is now available for purchase by anyone, including intelligence agencies. Online marketing datasets are a common example, and there are some published examples of US agencies purchasing such data. This can raise ethical and legal questions, not just about the use of the data for national security and law enforcement, but about ways such datasets might be used to manipulate views and public debate, as we saw during recent US election periods, including the actions of firms such as Cambridge Analytica. In another sphere, commercial satellite imagery and remote sensing datasets mean that a wide range of accessible geospatial data is commercially available without needing to task specialised, and expensive, satellite systems.

As a result, there are significant volumes of potentially valuable data available to the intelligence community even without the need for specialised 'covert source' collection capabilities that have traditionally been the agencies' main stock in trade. This is not to minimise the need for such capabilities, and such 'secret data' may often be key to intelligence activities, but as part of overall data collection, not as an end in itself.

While this observation is a truism, it's uncomfortably also true that control of and access to some open-source data is becoming increasingly difficult. This isn't just about the ubiquitous impacts of encryption, but also about how data is being controlled in countries such as China and Russia. At times, particular collection capabilities are 'going dark', while the technological and human reach of states such as China—and Russia in the cyber and disinformation spheres—is growing.

In this new environment, the role of intelligence agencies has morphed from collecting 'golden nuggets' of focused information (for example, the location of a key military asset) to making sense of the bigger picture. Strategic advantage will come from being able to link disparate pieces of information in order to understand the overall environment, and the intentions and decision-making processes behind what the adversary will do, not what they did.

In addition to occasional golden nuggets of individual facts, mass data analytics can discern value from the patterns and meaning within disparate datasets.

Advances in data analysis and data science, in particular artificial intelligence and machine learning, provide opportunities for the intelligence community to extract knowledge and insight from the data available to it. The question is about how much of that opportunity agencies will seize, how actively or reluctantly, and when.

Concepts such as neural networks have been around for decades but have now gained practical utility through the combination of increased computing power, the availability of datasets for training and testing, and improvements to algorithms. As a result, we see everyday applications that automate tasks we would have considered impossible a few years ago; for example, translation between different languages with usable levels of accuracy (if not of the quality that a trained linguist can provide).

But the digital challenge to intelligence agencies varies from mission to mission. Some missions, such as counterterrorism, have a broad global footprint and common data-collection and analytical challenges despite the disparate human terrain and the historical and geographical dynamics that shape the counterterrorism environment differently in the Middle East, across the Indo-Pacific, and in Europe, North America and Australia.

The combined challenges of the China mission, arising out of the nature of the Chinese state, its domestic controls and its technological development, require distinct approaches from the intelligence community. In some ways, the burgeoning digitisation of the Chinese economy and state result in multiple digital vulnerabilities, some from the fragmented and patchwork-like nature of the Chinese provincial and central government system and the various different developments of interacting digital systems that result from that, and some from the opposite dynamic towards reasserting the centrality of CCP and peak leader control, which includes the aggregation of national data for central government use. The CCP's attempts to strengthen control of itself (and its 90 million plus party members) and of the Chinese corporate and social worlds through technology incorporate all the digital vulnerabilities being experienced in other parts of the world, but perhaps to a greater degree.

In parallel, the Chinese state is seeking greater data security and greater data sovereignty (which also applies extraterritorially to Chinese firms' data, as well as to foreign firms operating in mainland China). This trend is moving in the opposite direction to China's overt policy of 'reform and opening up' and is better understood as an attempt at a 'great closing' of Chinese data to the wider world, except for the curated, managed data that state authorities choose to have released.

The economic decoupling that's been growing since the overt acknowledgement of strategic competition in technology between the US and China during the Trump administration provides a further distinct element of the systemic China challenge.[24] Communications, internet technologies and other high technology growing out of the digital world are the core focus for decoupling, even as broader decoupling between China and the major democratic powers seems likely to broaden in ways that were 'unthinkable' only two years ago.

The bifurcation of high technology and digital systems between China, its 'technology customer base' in major parts of the Indo-Pacific and Africa and the alternative technology bases of the G7, Quadrilateral Security Dialogue and AUKUS economies means that the intelligence community needs access techniques and particular technological and knowledge solutions that apply to the China mission that are different from approaches that work in other parts of the world. It's almost certain that success in the China mission will require the combined strengths of the different 'ints'—SIGINT, HUMINT, OSINT and IMINT[25]—with some echoes of approaches used for denied areas during the Cold War. However, the compound vulnerabilities that are a necessary attribute of the broad digitisation China is experiencing, and the complex human terrain of the enormous, diverse and fractious population and the authoritarian party controlling it, provide pathways for intelligence that the Soviet Union did not.

This is an extraordinarily rich if difficult time to be in the intelligence community, whether in Australia or in our key allies and partners.

… and intelligence tradecraft also needs to change

The intelligence profession has long focused on generating insights for decision-makers by providing access to secrets that others don't know or others seek to protect, while dealing with continuing uncertainties.[26] In this case, intelligence is about something knowable but known only to a small group. Providing access to such 'secrets' has over time been critical to decision-making in many government endeavours.[27] Indeed, historically, intelligence agencies have been critiqued for the secrets that they haven't uncovered.

More recently, the ability to collate and fuse the larger datasets that intelligence agencies have collected has become increasingly important. Imagination remains critical to future-focused assessments but increasingly comes second to sense-making through the application of artificial intelligence and self-learning algorithms developed to find 'secrets'.[28] Those secrets are obscured and embedded in large datasets rather than being locked in someone's safe.

While the strong demand for 'secret' intelligence endures, there's also a genuine change in client requirements over recent years. While still demanding secret intelligence, customers seek intelligence products that solve complex economic, social, technological and geostrategic mysteries.[29] Mysteries are 'unknowable', often unpredictable and not necessarily understood; nor is there any single 'secret' held by anyone that will help solve them. Still, careful data collection and analysis can reduce some of the uncertainty in mysteries. While the strengths of HUMINT may provide more contextual intelligence than other technical collection capabilities in these circumstances, neither can fully support the interpretation of mysteries.

There's been a paradigm shift in intelligence consumer demands that requires meaningful intelligence reform.[30] Secret intelligence and assessment face intense competition in today's dispersed media environment, and the intelligence community hasn't been quick to redefine its place and value proposition in this new context. Intelligence agencies must adapt to remain relevant and ahead of the increasing number of potential threats and the sheer velocity of events.

Tradecraft in intelligence collection and analysis must now change to exploit open data sources, and not just have 'open-source' centres running in parallel to traditional classified tradecraft and collection activities. And analysis must move away from more traditional inductive analysis. Reform of this type is a long and challenging process that must, in the Australian context, first overcome the national intelligence community's strong tribal cultures, which are so often resistant to change, along with the natural pride of intelligence professionals steeped in existing tradecraft. This is the 'industrial relations' aspect of change for intelligence.

The prioritisation of open sources doesn't mean an end to specialist covert data collection. Rather, it creates an enhanced opportunity for combining secret and open-source data to develop new insights. It's critical to note that doing so is legally and ethically complex in today's data-rich environment, but not doing so is a path to being surprised by events and actions, instead of producing insights for policy- and decision-makers that help them shape those outcomes. Hard intelligence targets, such as the inner secrets of the Zhongnanhai leadership compound in Beijing, will remain just that, despite volumes of data. And the China mission, in particular, along with the North Korea, Russia and Iran missions, will require techniques like those that have succeeded in making other denied areas at least partially known in the past. HUMINT will remain powerful, despite the complexities of identity management

and remaining covert. And, as was the case during the Cold War, the power of metadata in the SIGINT world, where messages' content might remain secure but accompanying data about the messages gives powerful insights through patterns and flows, is an obvious analogy to apply to such hard targets.

However, a clear difference from the USSR mission during the Cold War is the enormous and diffuse digital environment, particularly in mainland China. Despite the Great Firewall and current efforts to onshore and secure Chinese data, inherent vulnerabilities exist in the most capable digital systems and in the seams between systems. And seams are an unavoidable part of China's digital infrastructure that come with the structural nature of central and provincial authorities and the combination of their systems with commercial and state-owned enterprise systems. Offshore instances of Chinese technologies and corporate presence further complicate Chinese state security efforts.

Separately from access to data and insights from within mainland China or from Chinese systems, the availability of numerous commercial systems and data flows that provide insights into those otherwise restricted areas will be helpful for the China mission. Commercial satellite imagery of Xinjiang is an example.

It's an obvious but still necessary observation that the China mission will demand highly effective collaboration and burden sharing inside the Australian intelligence community and with its capable partners in the Five Eyes and in other places that have a common sense of urgency and priority for the China mission. Supporting minilateral cooperation through groupings such as the Quad and AUKUS is a role here.

In summary, the technological changes of recent years mean that the collection of data is no longer the key enabler of intelligence tradecraft. Data is everywhere, and the role of covert data collection supplements tradecraft but isn't an end in itself. The challenge is to work out which data is valuable, aggregate data that has utility and establish an effective data value chain to extract information, insights and knowledge from that data. In this new paradigm, intelligence agencies need to be able to do some specialised collection of data that fills in the gaps and obtains rare data that others don't have, along with the ability to effectively process and analyse all the data potentially available to them in a timely manner. But raw data by itself is unlikely to generate the 'insight returns' to justify this as a primary intelligence community focus because of the obvious utility of insights from widely available datasets, as demonstrated by powerful tech firms, states that are adopting these approaches at speed, capable individuals and new technology entrants.

For the national intelligence community, this evolving operating context isn't all good news. Traditional intelligence disciplines such as GEOINT (geospatial intelligence) face new competitors capable of leveraging the power of rapid technological advances. Data proliferation presents increased risks of compromises of HUMINT and makes the use of assumed identities increasingly difficult. Security intelligence and personnel security are faced with increased vulnerabilities to exploitation. The pace and cost of this change will present ongoing challenges across the intelligence community.

Given this, intelligence communities that have long relied on traditional tradecraft and means of collection and are averse to risk taking need to change. They must adapt to the changing tradecraft context and become more agile.

The ONI and the Australian intelligence community

Australia's national intelligence community is a very diverse construct. Its members are:

- three large agencies: the Australian Signals Directorate (ASD), the Australian Security Intelligence Organisation (ASIO) and Australian Secret Intelligence Service (ASIS)
- a small portion of two large organisations: the intelligence functions of the Home Affairs Department and the Australian Federal Police
- a group of smaller specialist agencies: the Australian Criminal Intelligence Commission, the ONI and AUSTRAC
- specialist portions of the Defence organisation: the Defence Intelligence Organisation and the Australian Geospatial Intelligence Organisation.

L'Estrange and Merchant's 2017 Independent Intelligence Review set the conditions for the Australian Government to establish the ONI and the Director-General of the ONI. In response to the review, the government built on the role of the Office of National Assessments, renaming it as the ONI. But, more importantly, the ONI was given national intelligence community enterprise management functions, promoting collaboration and coordination between the member agencies in order to enhance collective national security outcomes. This has included defining the key intelligence missions, aligning national intelligence agencies' activities in support of those missions, and ensuring that the intelligence community has the technical capabilities to deliver the required outcomes and that there's a suitably skilled workforce.

A key initiative from the Independent Intelligence Review was the establishment of the Joint Capability Fund,[31] which is administered by the ONI to procure and develop capabilities on behalf of the national intelligence community. While very few details about the level of funding or programs supported by the fund have been made public, in recent months the ONI has approached the market for commercial providers of services to the intelligence community as a whole. For example, requests for information have been published on AusTender for the provision of highly secure cloud services[32] and for intelligence analyst training programs.[33] The ONI has also led a grant program to engage with academia and research organisations to boost innovation and support national intelligence and security research in Australia. This aims to provide $18 million in funding to help deepen understanding of emerging science and technology to address intelligence and national security interests.[34] These are welcome, if small-scale, developments and seem to be working in a gap where there's obvious value in deeper collective operation by the intelligence community.

It's important to note that, like its US counterpart, the ONI has no limited authority over the other national intelligence agencies and no 'power of the purse' beyond its limited funds described above. Its remit to lead the national intelligence community is very much as a 'first among equals'. The Director-General of the ONI has the power to convene the national intelligence community and reports directly to the Prime Minister on the state of the community; however, he has no operational control over the other agencies, and the ONI therefore has to seek to achieve collaboration and cooperation across the national intelligence community by demonstrating mutual benefits to all participants.

The ONI also has convening powers to bring the intelligence community together to manage the national enterprise. And, because its Director-General reports directly to the Prime Minister on the state of the community, it has a way of influencing things beyond formal authorities.

Interestingly, another Independent Intelligence Review recommendation accepted and implemented by the government was to establish a joint capability fund.[35] As highlighted above, the ONI has been very busy producing capability on behalf of the national intelligence community in the public domain.

The ONI's challenge

Fundamental changes to intelligence clients' requirements and the intelligence mission have occurred in parallel with the changing strategic context, affecting the scale and scope of intelligence missions for intelligence enterprises. Those changes are the catalyst for what must be transformational reform of intelligence tradecraft. The transformation required here demands a rethink as significant as is necessary to meet the new strategic context. Without a doubt, this challenge has a technology dimension, but the stumbling block isn't so much technology as one of behaviour and psychology—rather than the woollier, hard-to-grasp notion of 'culture'.

Technology will continue to change, and the intelligence mission will evolve even without active decision or design. Still, each national intelligence community member has a strong institutional identity, statutory obligations and sets of behaviours—affected by its leadership at the time—and commitment to its respective tradecraft. This diverse set of institutional behaviours and tradecraft will not by itself futureproof the intelligence community. The challenge for the ONI centres on how to promote the kind of agility and collaboration that will catalyse the intelligence community's evolution to meet current and future geopolitical and technical tests. At times, this will mean driving the intelligence community in directions that even powerful individual agencies aren't going to move by themselves.

There's fierce agreement at senior ranks of the national intelligence community that collaboration and greater agility are critical to the future of the community and its broader mission. However, that agreement doesn't always result in action in a federated intelligence community, especially when budgets and independence are in play.

The ONI's relatively new enterprise management role is difficult and requires more than reliance on willing and collegial cooperation. The temptation for the community is to look to its partner agencies and communities in the UK and US for an appropriate model or template. The following sections illustrate that, while studying both nations' approaches will bring insights, they, too, face similar challenges and have their own constraints and institutional histories and dynamics. Clearly, as Australia's intelligence community draws on insights from its partners, it can't simply and dogmatically follow their lead.

The UK experience: ‘Collaboration from common purpose’

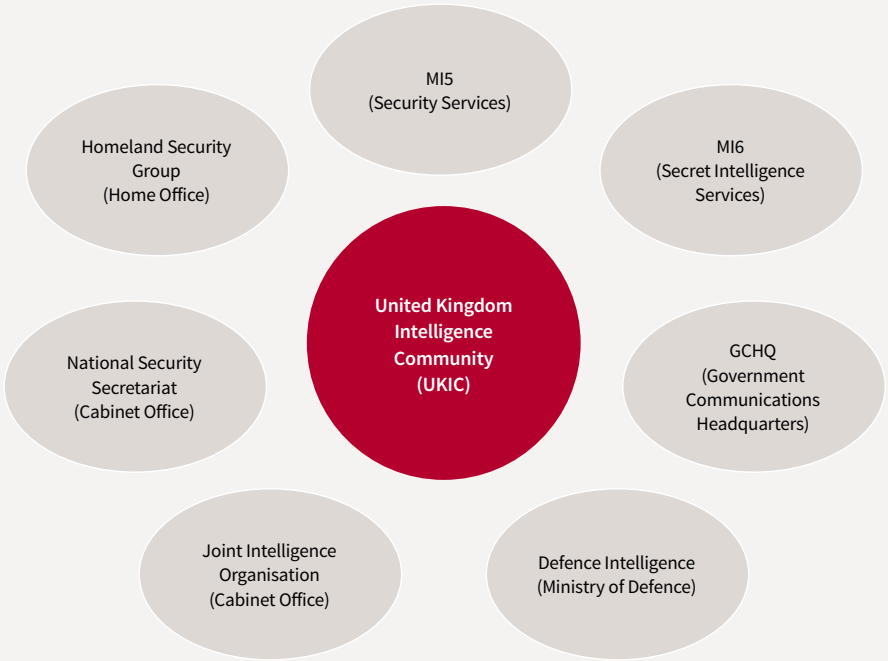
Drivers of collaboration

In Europe, by the late 1990s, the Cold War was a distant memory, the first Gulf War was over, and an end was in sight to the troubles in Northern Ireland. It did appear to be the beginning of a new era of long-desired strategic stability for the UK Government. Little surprise then that the Prime Minister, John Major, saw fit to cut deep into the nation’s intelligence budget at the end of the Cold War.

Elected in 1997, Prime Minister Tony Blair was committed to fiscal constraint.[36] The nation’s newfound era of peace and stability meant that the UK Government began to view its extensive, highly specialised and siloed intelligence community as an expensive insurance policy with little justification in terms of existential or other threats. Without a clear or perceived existential threat, Blair’s government argued that the UK intelligence community and security apparatus needed to be more fiscally constrained.[37]

The UK Government’s early budget cuts found savings and seeded greater competition between MI5, MI6 and the Government Communications Headquarters (GCHQ). Even before those measures, there was a silo between HUMINT and SIGINT in the UK and between domestic and foreign intelligence (Figure 5). Initial cuts exacerbated existing tribalism and grew intelligence agency competition. By the early 2000s, there was a low base of collaboration and little to change the trend.

Figure 5: UK Intelligence Community



Source: ASPI.

The UK intelligence agencies continued to experience funding constraints throughout the early 2000s that would intensify further in the latter half of that decade. Rather than budget reductions, there was growth, but with pressure for efficiencies to be realised.[38] At the time, it had become evident to the intelligence community's leaders that greater collaboration was needed, but knowing the need for change is very different from making change, as everyone can be dominated by the demands of business as usual and find it hard to make room to create and drive a transformation agenda. This means that it often takes an external trigger to catalyse change.

The second Iraq War, or, more specifically, its fallout, was a watershed moment for the UK intelligence community that would leave a stamp for a decade and a half. Seven years of rolling reforms and the now infamous Chilcot Report left the people serving in the UK intelligence agencies with a clear understanding that they needed to work together.

A trigger for greater combined mission focus, tragically, came on 7 July 2005, when four suicide bombers with daypacks full of explosives attacked central London, killing 52 people and injuring hundreds.[39] In seeking to understand why the attacks weren't prevented, the Greater London Authority found that the approach of individual agencies working in isolation was limiting their ability to 'join the dots' and identify key threats—similar lessons to those the US drew from 9/11, but much more tangible for UK agencies, given that the attacks happened in London. This led to the realisation that a joint approach across agencies, fusing onshore and offshore insights, was needed to deliver the mission.

That focus on joint mission success remains the key driver today, but along the way the momentum was undoubtedly helped by the need to respond to further austerity measures.

In 2010, Prime Minister David Cameron implemented a range of new austerity measures across the government.[40] Those measures again put agencies under intense downward budget pressure and drove the search for efficiencies. The fiscal pressure led to a range of changes. As well as inefficiencies within individual agencies, the government also identified overlaps between agencies and opportunities to rationalise approaches in a broad range of areas, including the management of major contractors, research and development, and the sharing of capabilities, skills and data. This 'common services' agenda is familiar in the wider public service environment in Australia.

Then, in 2020, Covid-19 became the catalyst for different ways of working, enabling more work at lower classifications and working from home.

The approach to collaboration

First, it should be noted that in the UK cross-agency collaboration is focused on the 'big 3' agencies: GCHQ, MI5 and MI6. No one person or organisation internal or external to those three agencies is appointed to lead, or even to convene or facilitate—the organisations are simply expected to work together collaboratively. However, the UK Cabinet Office does have two deputy national security officers, one of whom has coordination responsibilities. The chair of the Joint Intelligence Committee, who, beyond that powerful role, has no wider intelligence community authorities, can still use the UK intelligence community's single budget as a policy lever. Of course, one can speculate that it's far easier to achieve consensus among three similarly scaled agencies than across the diverse community of 10 national intelligence agencies in Australia. The Cabinet Office provides another layer of direction and insight that UK agencies are shaped by.

Expectations and accountability are enforced by the apparatus of government through the mechanism of the Single Intelligence Account in UK Government finances. The account isn't just an aggregation of three separate budgets to help preserve operational secrecy, but a reflection of the fact that the three agencies are expected to work together first to agree on their joint funding bid and then to present the bid as a single submission for approval. The power of this single funding measure seems to provide a far greater incentive than the ONI's modest central funding bucket established through the 2017 Independent Intelligence Review.

Combined with collaborative working relationships at all levels through the agencies, this means that there's a focus on what's needed to deliver the joint mission outcome. This drives early thinking about what can be done more effectively by working together, compared to what's appropriate for individual agencies to work on separately. For example, each agency still has its own requirements for bespoke technical capabilities for its particular remit and operating environment. However, putting in place standardised design principles and identifying which components of technology are reusable not only helps to drive efficiency and cost savings but also, crucially, can assist in making agencies' capabilities interoperable.

The UK intelligence community's transformation was aided in no small part by clear executive leadership on collaboration. The transformation process resulted in a painful decade of change—especially for those who were comfortable with the way things had been. Several false starts made that change even more difficult. However, once it started, executive leadership teams across the intelligence community made their people feel like they were part of the mission and a broader team, not just transacting with other agencies.

Collaboration in action

Broader UK Government policy settings drove a focus on efficiency across the UK intelligence community even as the limited budget reductions from the end of the Cold War ended with funding growth after 9/11. This helped push moves towards shared services that might otherwise have been resisted more strongly by individual agencies. For security reasons, the precise details of shared activities are not in the public domain, but it's generally understood that they cover the full gamut, from finance systems to human resources, from skills development to technical capability development, and from data analysis to assessment and reporting.

It's also interesting to note that some of the collaboration in fundamental enabling areas brings not only direct cost savings but often indirect benefits that can be just as important, if not more so. For example, there's a common access card and security clearance system across the intelligence organisations, so it's easier for staff from one agency to visit another agency for informal discussions and maybe even some 'water-cooler' chat in passing, but still with some restrictions and controls. Meanwhile, a common human resources system and harmonised pay and conditions make secondments of staff between agencies much simpler. These things help build up people's working relationships and awareness of each other, which helps to break down the silos between agencies.

In 2015, the UK Government introduced the Joint Security Fund, which forced even closer collaboration.[41] This measure was a deliberate effort to ensure that the UK intelligence community was investing in the capability it needed. It also sought to speed up technology development cycles for the intelligence agencies. This investment approach, coupled with the counterterrorism mission experience following the London bombings, recognised natural leads in the community for specific missions. The approach recognised that the most successful projects have focused and well-defined scope and objectives—there needs to be an achievable and precise definition of what success is, such as to build a capability, to address an operational issue or to perform some other function.

In the UK intelligence community's new construct, technology remained a key driver, but analytics also became important. Each intelligence mission has very different technological and analytical needs, so technology platforms needed commonality at the base but with diversity on top. Those in charge quickly established that each agency may still need its bespoke technical capabilities due to unique requirements. However, standardised design principles and reusable technologies help efficiency and interoperability where appropriate.

There was a need for more data for both the counterterrorism and the foreign intelligence missions. The changes in the counterterrorism landscape and its international dimensions led to a greater collaboration between MI5 and GCHQ. It seems that almost all the UK intelligence community's missions had moved to multisource operations.

Collaboration and pull-through of capability from industry and academia has been critical. On the industry side, we’ve noted that the UK Government’s financial austerity measures in 2010 drove changes in engagement with industry partners. That included better leverage of overall scale and buying power to get better value from those relationships, but that was combined with setting up longer term collaborative partnerships with key trusted companies.

The UK Government has also established the Accelerated Capability Environment, which is a capability within the Home Office that seeks to solve fast-changing digital and technological challenges facing law enforcement and national security agencies.[42] It brings together expertise from industry and academia ‘to innovate collaboratively and deliver front line mission impact at pace’.[43]

The UK has also set up accelerators, such as the Cyber Accelerator.[44] Places are allocated by competition, based on responses to technical challenges that link to areas in which current capabilities are weak and new products are needed.

The UK Government established the National Security Strategic Investment Fund as its corporate venturing arm for dual-use advanced technologies. It’s a joint initiative between the government and the British Business Bank. The fund invests commercially in advanced technology firms, alongside other investors, supporting long-term equity investment (‘patient capital’), and harnesses the government’s unique technology expertise. Its objectives include accelerating the adoption of the government’s future national security and defence capabilities and the development of the UK’s dual-use technology ecosystem. The fund has been operating for less than two years but has already achieved some early success. The scheme isn’t concerned just with future capability development but is also a key policy lever to ensure the sovereignty of national-security intellectual property.

Intelligence community transformation is a continuous process, as is the case in the UK. There is, however, benefit in taking stock of where the UK intelligence community is today due to the successes that it has achieved in increasing collaboration and agility over the past decade.

The US experience: 'It's all about the budget'

Without a doubt, the US intelligence community has long been an enormous conglomeration of powerful, well- funded agencies with multiple internal relationships and connections, laced together from different sources of legal authority and funding (Figure 6).

Despite its various unsung successes and public failures (including the Japanese surprise attack on Pearl Harbor), it has long struggled to be a community rather than just a grouping of agencies with a common intelligence function. Scale, mission, culture, secrecy, competition and budgets have contributed to the numerous pockets of inefficiency and tribalism that have collectively siloed the community's development. That siloed development has inhibited collaboration between agencies and agility across the US intelligence community and its various missions, but has delivered powerful capability in mission lanes, with clear benefits to partners such as the community's Five Eyes counterparts.

The US sought to harmonise intelligence sharing following the 9/11 attacks in 2001, when the community's failure of collation and imagination contributed to intelligence failures that denied authorities the opportunity to disrupt the attacks.[45]

The US Government's efforts to harmonise its intelligence community over the past two decades have concentrated on legislation, leadership and budgets.

In 2004, the *Intelligence Reform and Terrorism Prevention Act* established the Office of the Director of National Intelligence (ODNI).[46] The Director of National Intelligence (DNI) serves as the head of the nation's 18 intelligence agencies and the US President's chief intelligence adviser. The government established the DNI to ensure that information and, more importantly, intelligence are neither lost nor missed within the US intelligence enterprise—a massive task that to be successful requires both substantial reform and technology investment.

After establishing the ODNI, the government quickly learned that the ability of the office to coordinate the activities of the US national intelligence community was more vision than reality.[47] When it came to getting the national intelligence agencies to accept the guidance of the DNI, nothing much really changed for more than a decade.

At its onset, the DNI had little to no authority to get the intelligence agencies to do much of anything not explicitly directed in legislation, federal statutes or presidential executive orders. Fortunately, over time, and with the assistance of congressional legislation, the ODNI gained authority over budget control. Budget control provided the basis from which the DNI could loosely manage this federation of the slowly increasingly willing.

Despite being almost 20 years old, the ODNI is still a work in progress. Current arrangements aren't fully effective, despite the *Intelligence Reform and Terrorism Prevention Act*, Executive Order 13388 (2005)[48] and the *Homeland Security Act* of 2002,[49] which mandate a baseline for intelligence sharing. One research respondent indicated that this has more to do with cultures of suspicion and with data proliferation than any gap in legislation or regulation.

Figure 6: US Intelligence Community

The Director of National Intelligence serves as the head of the Intelligence Community, overseeing and directing the implementation of the National Intelligence Program budget and serving as the principal advisor to the President, the National Security Council, and the Homeland Security Council for intelligence matters related to national security.

Working together with the Principal Deputy DNI and with the assistance of Mission Managers and Deputy Directors, the Office of the DNI's goal is to effectively integrate foreign, military and domestic intelligence in defense of the homeland and of United States interests abroad.

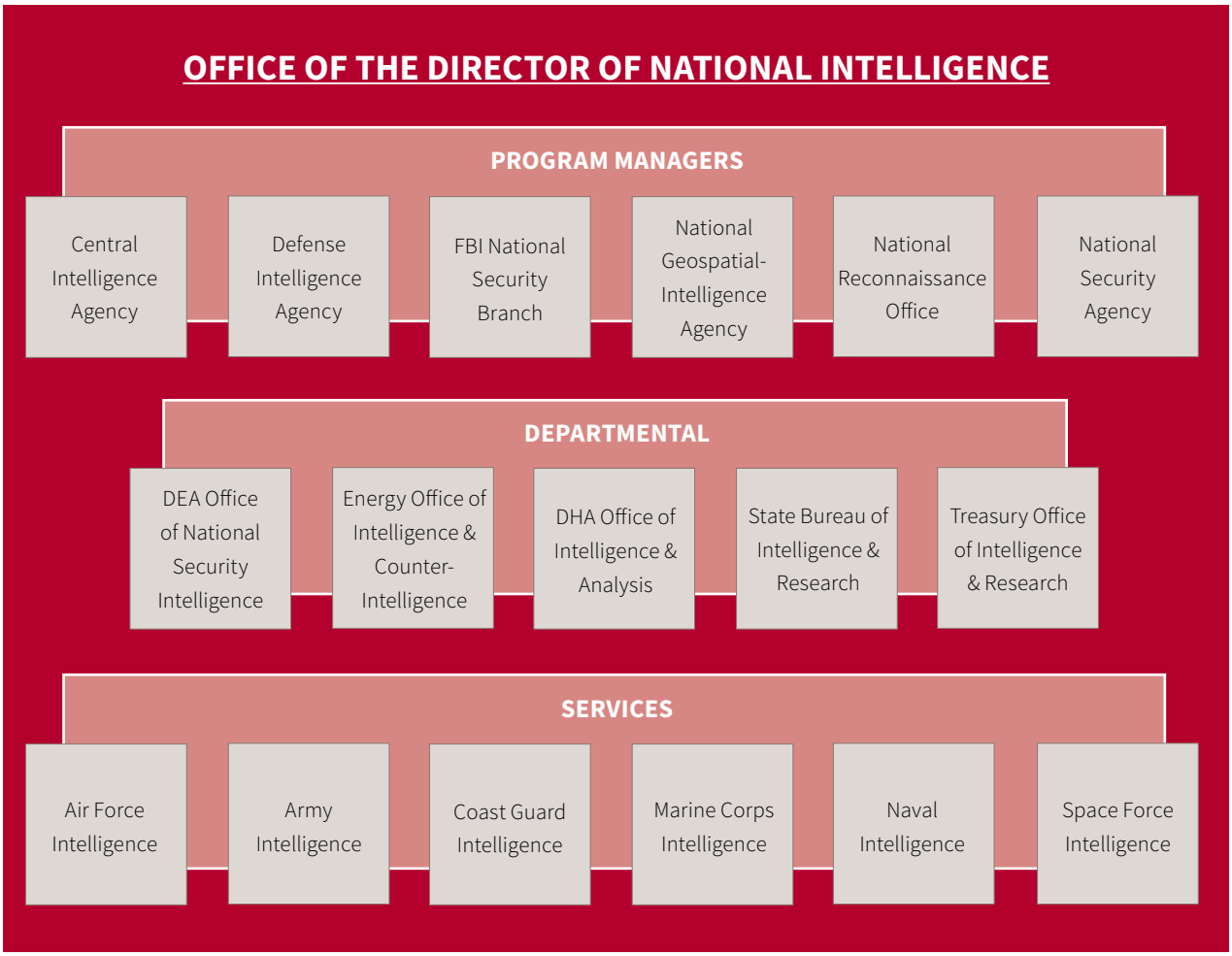
The U.S. Intelligence Community is a coalition of 18 agencies and organizations, including the ODNI. The IC agencies fall within the Executive Branch, and work both independently and collaboratively to gather and analyze the intelligence necessary to conduct foreign relations and national security activities

Source: Office of the Director of National Intelligence, online.

The IC's mission is to provide timely, insightful, objective, and relevant intelligence to inform decisions on national security issues and events. The DNI executes the IC's mission through decision making bodies, IC strategies, IC budget and resource management, development of IC capabilities, information sharing and safeguarding, and partnering with domestic and international partners

When it comes to the US intelligence community (or any intelligence community, for that matter), institutional policy and practices have a habit of driving thinking and behaviour. And, as is true in the Australian environment, those are tough to change. A research participant noted that more open-minded lower and mid-level managers are needed across the intelligence community to pull the community together. Much of its recent success is due more to its leadership's strength of character and personal perseverance, along with the drive and focus of the agencies' people, than to its 18 members having a shared vision (Figure 7).

Figure 7: US Office of the Director of National Intelligence



Source: The US Intelligence Community, online.

Interestingly, now that the ODNI's budget-control role has matured, the US intelligence community is beginning to work even more collaboratively on a range of critical challenges.

Research recipients reported that there's now a tremendous amount of collaboration across the intelligence community. After two decades of war on terrorism at home and abroad, the community is well positioned to deal with tactical intelligence fusion. The resurgence of Russia, the rise of China and increasingly belligerent rogue states, along with a dispersed but dangerous set of extremist actors, make the need for a collaborative, agile and strategically focused intelligence enterprise even more critical. Understandably, collaboration has moved away from focusing on the collection, sharing and dissemination of tactical intelligence to a higher (not necessarily broader) strategic level of direction.

At the heart of the US intelligence community's pursuit of more collaborative and agile strategic intelligence is a requirement to find new ways to bring classified data together with open-source bulk data. Secrecy, operational security and counterintelligence have served the intelligence community well in protecting its and collecting others' secrets. But, as we've highlighted, intelligence today is increasingly reliant on accessing and exploiting the best datasets and disseminating the subsequent analysis faster than opponents or those who might harm us.

There's long been competition between the various intelligence disciplines (HUMINT, SIGINT, MASINT[50] and so on) within the US intelligence community. That competition has been aided in no small part by the preferences and biases of intelligence customers. With the greater focus on datasets, not just the collection of 'secret' intelligence,

open-source intelligence has occupied an increasingly important space. While it's in its infancy, its future in the US intelligence community seems all but inevitable. However, its effectiveness may be predicated on the ODNI ensuring the application of appropriate technical skills and analytical tradecraft to its collection and exploitation and on its success in combining the open-source and classified datasets.

Cloud computing has become a critical capability within the US intelligence community. Due to the scale and diversity of its defence and intelligence agencies, the US has demonstrated different approaches to cloud adoption over the past 10 years. Various experiments by the Central Intelligence Agency (CIA) and the US Department of Defense (US DoD) have resulted in similar outcomes, but by widely different paths, some happenstance and a few unplanned events. That's been most obvious with the CIA's Commercial Cloud Enterprise (C2E)[51] and the US DoD's now-defunct Joint Enterprise Defense Infrastructure (JEDI) program.[52]

JEDI was a conceptual approach to creating a consolidated cloud infrastructure across the sprawling US defence community. It was developed to get ahead of and replace the burgeoning local experiments that, while individually promising, seemed likely to underdeliver on the overall capabilities possible through deep digitisation based on cloud approaches. A combination of tendering difficulty and political issues during the Trump administration slowed JEDI's implementation, and that gave local cloud approaches the opportunity to grow across the US DoD and the Defense intelligence enterprise. That turned out to be fortunate because, over in the world of the CIA, the approach to cloud infrastructure and services was moving from a single big cloud provider towards a 'multi-cloud, multi-vendor' approach. That change also turned out to be the way that the US big tech world was moving, in which the different technical offerings—and the 'app ecosystems' available in each—provide the advantage of diverse capabilities and give government agencies a way of retaining commercial leverage over their technology partners. The formal cancellation of JEDI means that the US DoD now has a multi-cloud, multi-vendor strategy, similar at least in concept to that of the CIA. That leaves it well positioned to take advantage of capabilities such as Microsoft's recent announcement of the general availability of top secret cloud services for the US Government, but not locked in to a single provider, with the inherent risk that involves.[53]

As with Australia and Australian interests, the newly emerged critical policy and intelligence issue is the systemic challenge posed to US interests by China across the broad and intermingled strategic, economic, technological, political and environmental domains. The political signal that this is the case is clearer under the Biden administration than under the preceding two US administrations, and was marked recently by three developments: the US withdrawal from Afghanistan; the deepening and accelerating of the role of the Quad at leadership level between the US, India, Japan and Australia; and the AUKUS agreement between the US, the UK and Australia. Interwoven challenges from climate change and its compounding effects, broader technological change and continuing issues such as violent extremism, domestic security and existing international security flashpoints complicate the US intelligence community's roles and priorities to a greater extent than in Australia, although the scale and reach of the US agencies compensates for that in many ways.

One quote from a US official about a particular technological development conveys the new mindset required for the China mission well:

> In the past, we put a lot of confidence in our assessment of what an adversary like China will do in the future and we use that to inform how we want to make our investments. One of the lessons I've taken from my own experience [is] that we should look at what is possible from a physics perspective, as opposed to what we think they're going to do, because China, again and again, has proven that if it is possible within physics and it will surface another hole in our swing that they will do it.[54]

Intelligence insights help avoid these kinds of surprises and mitigate their impacts and frequency.

For the UK, Australian and US intelligence communities, AUKUS is a major strategic development, although the work agenda for AUKUS is particularly focused on the accelerated development and deployment of a range of technologies into the defence and broader national security space, and a number of the AUKUS areas are already core to Five Eyes intelligence cooperation.

Observations and insights

So, what are the significant trends and insights from the very different US and UK intelligence communities that Australian policymakers and intelligence practitioners and leaders can bring to their environments?

1. Burning mission requirements drive transformative change in intelligence communities

Real, transformative intelligence community change is far more likely to result from a 'burning mission' requirement than from changed government policy, budget constraints or leadership direction—although those other factors certainly help to create the environment for change.

External drivers, such as the need to continue to operate during the pandemic, can also add momentum. Still, there must already be extant drivers for change that are underpinned by a desire for transformation. The UK, for example, experienced waves of budget cuts that started during the Blair government. Nevertheless, it appears that the fundamental shift towards interagency cooperation at speed and scale occurred because, without that, UK agencies risked failure in the driving counterterrorism mission in the aftermath of the July 2005 London bombings.

As in Australia, agency identities, structures and focuses are both advantages and obstacles. However, driven by the mission imperatives and focusing on the joint objectives required to achieve them, this has created a collaboration mindset that counterbalances those 'silos of excellence'. Where the mission imperative is strong enough, deeply integrated approaches to data sharing and combined workforce skill sets demonstrate potent results. For personnel who have experienced a rise into leadership roles, there's the promise that longstanding institutional and behavioural barriers to closer integration can be overcome, beyond the mission-specific exceptions we see now.

For Australian agencies, particularly those with a foreign intelligence focus such as ASD, ASIS, the Defence Intelligence Organisation and the ONI's assessment element, but also for ASIO in the area of foreign interference and counter-espionage, the China mission is that burning platform. Arguably, this grouping of agencies is the 'minilateral' within the larger national intelligence community that must combine most closely and urgently on the China mission, even if that complicates the 'all one community' concept of the broadened national intelligence community that was proposed in 2017.

The distinct attributes of the China mission outlined in this report require a distinctive approach as the high-technology decoupling between China, Australia, the US and other powerful democracies deepens. But there's enormous potential for success in this key mission because of that decoupling and the nature of the Chinese state. That comes partly from the CCP's increasing dependence on digitisation for domestic control and operations and from China's growing international technological footprint.

Lessons from dealing with denied areas during the Cold War era are relevant; however, the scale of data on mainland China available from non-intelligence means, such as commercial imagery, combined with the continuing strengths of human intelligence and the inherent vulnerabilities in multilayered, complex digital systems working through equally complex, unstable institutional structures, as we see in the party-state complex that makes up the Chinese regime, provide the seeds for mission success.

2. Sudden paradigm shifts can accelerate existing transformation programs

What's the pandemic ever done for us? Covid has delivered on the cliché 'never let a crisis go to waste'.

In the case of Covid-19, the immediate challenge of a sudden paradigm shift in the operating context appears to have forced agencies and their people to rethink the 'unthinkable' and break policy and process barriers that would otherwise prevent change.

In the UK, as in Australia, agencies rushed to disperse their workforces in response to Covid and to have limited personnel numbers in highly classified environments. That new approach led to a noticeable acceleration in 'low-side'[55] development activities by UK industry partners and agency personnel. Engineers were able to not just keep the lights on but continue to develop capabilities. It also allowed the 'build on the low side, deploy on the high' methodology, which might otherwise have taken many more years to finalise.[56] This change in the UK intelligence community was admittedly about engineers, not broader changes to the intelligence workforce, but has demonstrated the power of low-side applications and development. There's now a chance, almost a certainty, that low-side analytical work can also add value, even before combining low-side and high-side data as technology platforms allow that to happen.

3. Leadership is the key to driving collaboration and transformation

In the UK, the US and Australia, the different intelligence agencies have separate structures, mandates and reporting lines. However, if the leaders of those agencies set the tone in prioritising collaboration and focus on joint outcomes, that will permeate through their organisations, driving better integration and working relationships at all levels.

The US has had a model of a coordinating authority, the DNI, whereas the UK has taken a more collegial approach that involves no formal 'convenor' of the intelligence community. Both approaches have their own strengths and weaknesses—what's more important are the mindset and messaging from the individuals in leadership roles, rather than the precise structures and processes put in place to manage collaboration.

Of course, fine words from leaders also need to be backed up with actions, putting in place the right frameworks and processes that promote micro- and macro-collaboration. This includes enablers such as aligning human resources conditions, clearances, access passes and the like, and encouraging the right behaviour through measuring and assessing the degree of integration and collaboration with other agencies.

This leadership approach requires a shared understanding of the growing risks to individual agency (and intelligence community) success if behaviours don't shift to delivering insights from more common technology platforms and the exploitation of shared data, albeit leavened by agency-specific applications and (limited) bespoke data.

4. The intelligence community needs to embrace modern technology and keep up to date as it continues to advance

Due to a combination of the security constraints that intelligence agencies operate under, slow procurement processes and general inertia, the intelligence community isn't normally renowned for having the latest and greatest technology (despite what the spy dramas on TV might suggest). It does continue to have access to powerful systems and technologies and to have an ability to develop novel techniques that can deliver considerable success in particular areas.

However, the shift to low-side, remote working over the past 18 months has opened the eyes of intelligence community personnel and leadership to the clear advantages of using leading commercial development tools and infrastructure and identifying and applying applications and approaches from other fields of activity, and the demonstrations of that phenomenon in the UK are worth paying attention to.

So far, this report has been focused mainly on capability development, but there's also potential in the power of analyses of large-scale datasets on the low side. Our analysis also indicates that the real benefits of low-side, large-scale data and analysis will be maximised only when the technology platforms can accommodate it and when solutions are found that allow low-side insights (if not data) to be combined more easily with the unique classified data available to intelligence communities.

This links to another key insight: the benefits of adopting modern cloud-based architectures and solutions. The cloud isn't a silver bullet, and not even necessarily a cost saver, but it can be a major enabler of innovation and agility. However, the needs of the intelligence community are complex and diverse, and there won't be a single uniform cloud solution to all problems. The answer will need to be a 'cloud of clouds', at different classifications, from different vendors, with different features. Due to the scale and diversity of its defence and intelligence agencies and communities, the US has demonstrated different approaches to cloud adoption over the past 10 years. Put simply, the different experiments by the CIA and the US DoD have resulted in an endgame of multi-cloud, multi-vendor strategies, but by widely different paths.

5. Process and technology can only get so far—you need the right human capital to make things happen

As will be very familiar to the driven people inside Australia's intelligence community, it's the mission focus that makes the work so attractive and so satisfying. That's true whether those individuals are part of the intelligence agencies or are committed corporate partners.

The UK seems to show that the mission imperative that drives cross-agency teams to collaborate is powerful enough to create connections below the level of an agency's leadership that could even take integration further than the leadership may have intended. This dance between the competing imperatives of agency capability and influence and overall intelligence-community mission success appears to acknowledge and work with, rather than discount cooperation, mainly because the drivers of change in the way the community operates are likely to require the mission-focused approach to become more dominant.

But it also seems that the idea of empowering analysts and technologists to adopt approaches, tools and technologies and change the places where they work isn't enough. Both the US and UK experiences have featured unhealthy doses of 'resistance to change' within deeply capable analytical and technical communities. Those promoting major change need to be aware that, traditionally, professional self-regard, and often career progression, have come from becoming the leading expert in a particular niche, not from agency leadership—and the speed of change driven by technologies and approaches used by adversaries and capabilities available in the open-source world can be threats to that.

As well as the need to bring existing talent on the transformation journey, the intelligence agencies also need to attract more fresh talent with new skills, such as artificial intelligence and machine learning approaches, along with techniques such as data visualisation and data fusion to empower analysts and distil findings for decision-makers. Those technical specialists are of value (and will stay) only if the agency and government leaders and decision-makers are open to confronting and uncomfortable advice and have enough confidence to trust the advice of what, on occasions, can be staff in relatively junior or obscure roles. If they find themselves bouncing off the resistance of professionals who already 'know boats' and discount their expertise, then retention will be difficult and their impact will be limited.

A UK approach to low-side data analysis for intelligence purposes might be one path here. While low-side development activities have proceeded broadly during the pandemic, low-side analysis has been a case of several pilot projects in different parts of the intelligence community. This makes it possible for intelligence community leaders to adopt and expand successful 'pilots' more broadly and use the smaller pilot project teams to mix skills, backgrounds, agencies and cleared industry partners.

6. Private–public partnerships need work

Getting over the view that intelligence issues are unique and that industry partners' insights from their quite different corporate perspectives and operating environments are less valuable is essential—arguably all the time, but certainly right now at this time of rapid technological flux and intensifying strategic competition with adversaries that may have fewer constraints in this area than we do.

Interestingly, the UK experience with industry partners has paralleled internal changes in the intelligence community. As in the broader national security and defence worlds, UK agencies work deeply with trusted industry partners, who are in many ways part of the internal intelligence community workforce and technical capability. There are procurement policies and proprieties, of course, but the level of integration as capability partners seems high.

However, private–public partnerships take a long time to develop and mature and can be damaged in a moment. They can't be 'set and forget' arrangements: like any relationship, they need constant work on both sides to keep them relevant and mutually beneficial. The intelligence community also needs to understand that the Snowden leaks have generated a great deal of concern over possible corporate reputational risks associated with intelligence community partnerships for the corporates, and that will need to be managed.

7. Redefine open-source efforts

Narrowly, open-source analysis and competitive insights from the non-intelligence world are a challenge to agency influence and mission success. If decision-makers perceive that the information or insight advantage they obtain from expensive and highly classified intelligence agencies isn't large enough to justify the investment of resources (and decision-makers' time in using agencies' products), then that's an existential risk to any intelligence community. That risk has been increasing in recent years with the rise of big data and vast volumes of analysis—and commentary—from entities outside governments in the Five Eyes and the broader world.

The more considerable risk, though, to both the US and UK intelligence communities is not this 'insider risk' within their nations from competitive open-source intelligence. Instead, it's the risk that adversaries are creating and adopting capabilities, technologies, concepts and ways of working that can provide defining 'insight advantage' and allow their owning governments to operate within the decision cycles of Five-Eyes governments, and perhaps penetrate government systems and secrets as a result. This type of 'burning platform' mission imperative drives profound change in the UK and US intelligence communities. And the key adversary intelligence actors are Russian and Chinese agencies and their quasi-corporate and quasi-criminal partners.

Five Eyes intelligence clients need to move beyond their bias towards classified analytics. However, to do so requires that the insight advantage, especially that which leverages open-source data, is underpinned by the right technology, analytics and tradecraft.

Where to next?

In this report, we've paid particular attention to not treading the path of so many previous intelligence reviews and research projects and to offering recommendations of practices from the UK and the US that should be copied in Australia. However, the research process provided an opportunity to identify insights and ideas for the Australian intelligence community. While we acknowledge that many of this report's insights might already be at the front of the minds of those in intelligence capability roles, it's still prudent to identify some possible next steps.

It's almost certain that future intelligence successes will be the rewards for intelligence communities that:

- have the best datasets
- can leverage the combined value of both secret and open sources
- can exploit those datasets, collection capabilities and analytical processes fastest
- are open to the adoption of unfamiliar technologies and approaches from the world outside intelligence before such approaches proliferate to the level of obviousness.

Achieving that kind of success will be no easy task for intelligence communities in which data and capabilities are siloed between different agencies (and often within individual agencies) and many technologies and operating models are trapped in the paradigms of the past. The underlying causes are complex, and a range of solutions will be required to address them. However, we recommend five policy areas for consideration.

1. Leadership must focus on and drive integration across the national intelligence community

The broadening of the Australian intelligence community since 2017 has without doubt created new opportunities for collaboration and cooperation. However, other policy initiatives, such as the introduction of the Home Affairs portfolio and the Defence Intelligence Group, have also served to create new 'multilateral' collaborations, with all-new lines of control and, at times, politicisation.

The ONI should use its convening power to lead the Australian intelligence community in defining joint intelligence mission objectives and ensure a relentless focus on achievement of those joint outcomes as the primary measure of success for each of the community's constituent agencies. At the next level down, it should define metrics to measure collaboration and then coordinate the community to drive measuring and reporting of the metrics, and use them for agenda setting for cross-community discussions.

As well as a top-down approach, action is also needed from the bottom up. Encouraging and facilitating more staff mobility between agencies, both for permanent moves and for secondments, would help to build shared understanding. Even basic initiatives such as a common access pass system could be reconsidered in the light of the indirect benefits they could bring.

A focus on particular priorities for which broad intelligence-community data and reach can make defining differences seems more likely to succeed than attempting wholesale change to the community on the broadest front. More specifically, the China intelligence challenge is the burning mission of today, and, just as for counterterrorism, there's an opportunity to leverage that challenge as a driver for greater collaboration.

Getting collaboration on this mission across 10 very different organisations, in a timely manner, will be no easy task. Here the Director-General of the ONI could use his leadership role to create a new minilateral grouping of intelligence agencies focused on enhancing collaboration and cooperation.

The recent announcement of AUKUS could provide an additional opportunity for this minilateral group of intelligence agencies to enhance collaboration with the UK and US intelligence communities, although, as we've noted, the Five Eyes members have a deepening convergence on the systemic challenges of China, as we see with other key partners, whether in the Quad, the broader Indo-Pacific or Europe. International intelligence cooperation on China seems likely to be the subject of a number of complementary groupings.

2. Accelerate the adoption of modern technologies

Meeting the data and analytical challenge of ever growing datasets requires rapid access to leading-edge data capabilities. As an interim step, the intelligence community needs to work collaboratively to rapidly unleash the power of machine learning on the high side. The way it does that is important, as there's a need to avoid having individual agencies make sensible-sounding cases to do their own thing, while making comforting noises about doing so collegially.

The intelligence community needs to work collaboratively to rapidly unleash the power of machine learning on the high side.

This report and our previous cloud-computing paper (*National security agencies and the cloud: an urgent capability issue for Australia*[57]) both mention the importance of national security high-side clouds. The lesson for the future here is that the intelligence community needs to build for the cloud now, not for any interim solution that waits to see what comes next. Also, a common IT environment needs to be complemented by a common data environment, including frameworks such as a cross-community approach to data governance and standards.

One of the fundamental building blocks for achieving that data advantage is the elevation of these discussions from chief information officers (CIOs) and chief technology officers (CTOs) to the agency head, ministerial and National Security Committee of Cabinet level. To do so, strategists, policymakers, CTOs and CIOs must work to better educate senior decision-makers on bleeding-edge capabilities and their fundamental building blocks. It's likely that ministers and the National Security Committee will be relieved to hear of an increased appetite for change because of their appreciation of the speed of change in areas outside intelligence.

To actualise this approach, consideration needs to be given to how the Australian intelligence community acquires capabilities. To date, each member of the community has operated its own acquisition capability, with much variation between agencies and little cross-community collaboration. There's an opportunity to address this, at the very least to consider issues such as common software licences. A far bolder approach could include the sharing of common procurement capabilities using a strategic partner acting as a managing contractor.

Strategists, policymakers, CTOs and CIOs must work to better educate senior decision-makers on bleeding-edge capabilities and their fundamental building blocks.

3. The approach to open-source intelligence needs to be transformed

We see a clear demand for an enhanced, or even a complete, reconceptualisation of open-source intelligence. While open-source collection and analytical capabilities of various complexity exist among the Five Eyes partners, there is, for the most part, a lack of a centre of gravity that would see its full exploitation. Our research, and its participants, noted that open-source intelligence requires more use cases. With those use cases, a collection and analytical tradecraft can be developed that ensures the validity and reliability of this mission-critical intelligence source.

It also requires a reconsideration of data exploitation from open sources and a far more robust and secure low side that protects intelligence collection requirements and gaps.

A collection and analytical tradecraft … needs to be developed.

There are already well-developed discussions about leveraging greater intelligence value from open sources and the increasing demands for the data workforce. To date, those ideas have coalesced around two different approaches. The first involves the establishment of a new open-source intelligence agency that services intelligence clients and analytical agencies. The second response consists of the pooling of the precious open-source collection and an analysis of human capital (for example, data scientists) from across the community within a single existing entity that prioritises the allocation of those resources. It's probably going to be of greatest value to analysing open source and high side data together, rather than doing separate analysis and combining the fruits. Regardless of which path is selected, it appears abundantly clear that a collaborative intelligence-community response is required.

But building an open-source silo is almost certainly the wrong approach, given the power that should flow from combining those large, more readily available datasets with the more sparse and hard-to-obtain classified data that for decades has been the foundation of intelligence analysis.

4. The intelligence community needs to look outside the bunker and work more effectively with industry and academia

The intelligence community faces some unique and complex challenges, and has some of Australia's best and brightest minds to help solve them, but it can learn much from 'outsiders' in industry and in academia. The routes to achieve this can take a number of different directions, from drawing on outside organisations as a source of labour resources to adapting or even directly using existing intellectual property and products.

This could be facilitated by creating shared spaces in which government, industry and academia can work together to address intelligence challenges at an unclassified level, or at least at lower classification levels. We've previously noted the need for the intelligence community to embrace the cloud, and that could be another benefit of working together.

While having the right infrastructure and other enablers will help, fundamental institutional and behavioural change will be needed to foster the right partnerships and dialogue. That starts with a better appreciation from within the intelligence community of the way that commercial organisations work, their drivers and their challenges. Australia could learn from the UK experience of secondments of public servants to work as embedded staff in commercial organisations. That would help to build shared understanding, as well as providing other benefits from the cross-fertilisation of approaches and ideas.

5. New structures are needed to develop the breakthroughs needed for the future

There's already a tremendous amount of high-quality research being undertaken and sponsored in agencies, especially those charged with technical intelligence collection and analysis, in each of the Five-Eyes intelligence communities. Much of that research focuses on meeting immediate or near-term intelligence challenges: it's concerned with incremental advances rather than transformational change.

For 60 years, the US Government has funded the Defense Advanced Research Projects Agency (DARPA) to make pivotal investments in breakthrough technologies for national security. The US also operates the Intelligence Advanced Research Projects Activity (IARPA). An Australian IARPA, focused on the intelligence community's challenges, could have the economy of scale to ensure a transformational change in those communities. It's critical to note, however, that IARPA-type arrangements have been focused on the long term and more often than not have produced results in slow time. The key to the success of an IARPA-type arrangement is finding the right problems that require research and transformational change. And, just as for private–public partnerships, serious thought needs to be given to intellectual property ownership.

Conclusion

Australia's national intelligence enterprise is facing a rapidly changing operating context. In the deteriorating strategic environment, intelligence consumers are less interested in secret intelligence from single sources than they are in insights that help them make decisions, from whatever source. Intelligence that reduces the uncertainty of decision-making in a dangerous and complex world remains highly valued. The new environment, notably shaped by a technologically adept and assertive Chinese state with reach across its corporate and technology worlds, is set to have a transformative impact on intelligence communities, as are the other primary drivers of change noted at the start of this report: Covid, climate change and technology. If intelligence communities fail to adapt to those changes, they risk becoming irrelevant and falling behind state and non-state threat capabilities.

In this environment, collaboration and agility should be far more than an aspirational vision statement. Instead, both ought to lie at the core of ensuring that the Australian intelligence community can secure and leverage the best datasets, regardless of their classification. The traditional 'fusion' approach to bringing the high and low sides together isn't the answer. Instead, leadership and mission focus are needed to leverage the total value of the various intelligence disciplines: SIGINT, HUMINT, IMINT, MASINT and so on.

Agility will come from bringing about the institutional and technological changes that allow for the rapid development of new capabilities. The 'build on the low side, deploy on the high side' mantra found in SIGINT agencies is a start, but we still need more.

What's abundantly clear from this research project is that the control of intelligence budgets, whether dispersed or centralised, isn't a sufficient driver to pull down the tribal silos. Interestingly, a clear mission with a more centralised or shared budget sharpens collaboration, leading to lasting change. Australia's intelligence community faces just that sort of challenge right now. Today's strategic uncertainty creates the burning-platform intelligence mission that's needed to force change.

There's no magic potion for futureproofing Australia's intelligence community. Nor should Australia simply look to Five-Eyes partners such as the US and the UK for cookie-cutter solutions to determine how to best position for the intelligence challenges of today and tomorrow. That's why this report has instead focused on identifying insights from US and UK experience that may have utility for Australia.

Notes

1 Michael L'Estrange, Stephen Merchant, *2017 Independent Intelligence Review*, Department of the Prime Minister and Cabinet, 18 July 2017, online.
2 Patrick F Walsh, 'Transforming the Australian intelligence community: mapping change, impact and challenges', *Intelligence and National Security*, 2021, 36(2):243–259, doi: 10.1080/02684527.2020.1836829.
3 Office of National Intelligence (ONI), 'The national intelligence community', Australian Government, no date, online.
4 Graeme Dobell, 2020, 'The making of the Australian intelligence community', *The Strategist*, 15 June 2020, online.
5 Attorney-General's Department (AGD), *Report of the Comprehensive Review of the Legal Framework of the National Intelligence Community*, Australian Government, 4 December 2020, online.
6 AGD, *Report of the Comprehensive Review of the Legal Framework of the National Intelligence Community*.
7 ONI, 'Forming a national intelligence community', Australian Government, no date, online.
8 Department of Defence (DoD), *2020 Defence Strategic Update*, Australian Government, 1 July 2020, online.
9 TJ Ma, RJ Garcia, F Danford et al., 'Big data actionable intelligence architecture', *Journal of Big Data*, 2020, 7:103, online.
10 Kjetil Anders Hatlebrekke, *The problem of secret intelligence,* Edinburgh University Press, Edinburgh, 2019.
11 Rajiv Shah, *Working smarter, not harder: leveraging government procurement to improve cybersecurity and supply chains*, ASPI, Canberra, 18 August 2020, online.
12 L'Estrange & Merchant, *2017 Independent Intelligence Review*.
13 DoD, *2016 Defence White Paper*, Australian Government, 2016, online.
14 DoD, *2016 Defence White Paper*.
15 L'Estrange & Merchant, *2017 Independent Intelligence Review*.
16 John Coyne, Peter Jennings (eds), *After Covid-19: Australia and the world rebuild* (volume 1), ASPI, Canberra, 2 May 2020, online.
17 Lesley Seebeck, 'Zeroing in on the grey zone in the Indo-Pacific', *The Strategist*, 24 June 2021, online.
18 Fergus Hanson, Emilia Currey, Tracy Beattie, *The Chinese Communist Party's coercive diplomacy*, ASPI, Canberra, 1 September 2020, online.
19 'National security', Australian Parliament, 4 December 2008, online.
20 Daniel Hurst, 'Federal government tears up Victoria's Belt and Road agreements with China', *The Guardian*, 22 April 2021, online.
21 Heather Ashby, 'Far-right extremism is a global problem. And it is time to treat it like one', *Foreign Policy*, 15 January 2021, online.
22 'Great power competition and cyber conflict', symposium, Council on Foreign Relations, 7 January 2020, online.
23 Barnett S Koven, 'Responding to gray zone conflict: countering Russia in the Donbas and beyond', *Small Wars Journal*, 6 July 2021, online.
24 *National Security Strategy of the United States of America*, The White House, December 2017, online.
25 SIGINT = signals intelligence; HUMINT = human intelligence; OSINT = open-source intelligence; IMINT = imagery intelligence.
26 William J Lahneman, 'The need for a new intelligence paradigm', *International Journal of Intelligence and CounterIntelligence*, 2010, 23(2):201–225, doi: 10.1080/08850600903565589.
27 Hatlebrekke, *The problem of secret intelligence*.
28 CSIS Technology and Intelligence Task Force, *Maintaining the intelligence edge: reimagining and reinventing intelligence through innovation*, Center for Strategic and International Studies, January 2021, online.
29 CSIS Technology and Intelligence Task Force, *Maintaining the intelligence edge: reimagining and reinventing intelligence through innovation*, Center for Strategic and International Studies, January 2021, online.
30 CSIS Technology and Intelligence Task Force, *Maintaining the intelligence edge: reimagining and reinventing intelligence through innovation*.
31 L'Estrange & Merchant, *2017 Independent Intelligence Review*.
32 AusTender, 'Request for expressions of interest for the provision of highly secure private community cloud services', Office of National Intelligence, 11 December 2020, online.
33 AusTender, 'Request for information (RFI) for the design, development, delivery of the Intelligence Analyst learning experience', Office of National Intelligence, 8 April 2021, online.
34 ONI, 'Research funding to address intelligence and national security threats', Australian Government, no date, online.
35 L'Estrange & Merchant, *2017 Independent Intelligence Review*.

36 Malcolm Sawyer, 'Fiscal policy under New Labour', *Cambridge Journal of Economics*, 2007, 31(6):885–899, online.
37 'Brown "ignored last Iraq inquiry and cut budget for intelligence"', *Evening Standard*, 12 April 2012, online.
38 Nick Ritchie, 'Rethinking security: a critical analysis of the Strategic Defence and Security Review', *International Affairs (Royal Institute of International Affairs 1944–)*, 2011, 87(2):355–376, online.
39 Greater London Authority, *Report of the 7 July Review Committee*, June 2006, online.
40 Nicholas Watt, 'David Cameron makes leaner state a permanent goal', *The Guardian*, 12 November 2013, online.
41 Frank Gardner, 'Budget 2015: What is the new Joint Security Fund?, *BBC News*, 9 July 2015, online.
42 Home Office, 'Accelerated Capability Environment (ACE)', UK Government, no date, online.
43 Home Office, 'Accelerated Capability Environment (ACE)'.
44 National Cyber Security Centre, 'Overview', UK Government, no date, online.
45 9/11 Commission, *The 9/11 Commission report*, 22 July 2004, online.
46 Civil Liberties and Privacy Office, *Intelligence Reform and Terrorism Prevention Act of 2004*, Office of the Director of National Intelligence, US Government, no date, online.
47 Office of the Director of National Intelligence, 'Mission, vision and values', US Government, no date, online.
48 'Executive Order 13388 of October 25, 2005: Further strengthening the sharing of terrorism information to protect Americans', The White House, online.
49 Homeland Security Act of 2002, Public Law 107-296, US Congress, 25 November 2002, online.
50 MASINT = measurement and signature intelligence.
51 Jason Miller, 'As C2E gets going, DIA sets its strategy for more cloud services', *Federal News Network*, 9 April 2021, online.
52 Department of Defense, 'Future of the Joint Enterprise Defense Infrastructure Cloud contract', media release, US Government, 6 July 2021, online.
53 Tom Keane, 'Azure Government Top Secret now generally available for US national security missions', *Azure*, 16 August 2021, online.
54 Patrick Tucker, 'China's hypersonic test raises questions about US missile defense, deterrence', *Defense One*, 19 October 2021, online.
55 'Low-side' refers to a government network that is used to process, store and or communicate lower classified or unclassified information.
56 'high-side' or 'on the hign' refers to a government network that is used to process, store and or communicate highly classified information.
57 John Coyne, Michael Shoebridge, Albert Zhang, *National security agencies and the cloud: an urgent capability issue for Australia*, ASPI, Canberra, 27 May 2020, online.

Acronyms and abbreviations

ADF	Australian Defence Force
ASD	Australian Signals Directorate
ASIO	Australian Security Intelligence Organisation
ASIS	Australian Secret Intelligence Service
ASPI	Australian Strategic Policy Institute
C2E	Commercial Cloud Enterprise
CCP	Chinese Communist Party
CIA	Central Intelligence Agency
CIO	chief information officer
CTO	chief technology officer
DARPA	Defense Advanced Research Projects Agency
DNI	Director of National Intelligence, US
DoD	Department of Defense, US
GCHQ	Government Communications Headquarters, UK
HUMINT	human intelligence
IARPA	Intelligence Advanced Research Projects Activity
IMINT	imagery intelligence
JEDI program	Joint Enterprise Defense Infrastructure program, US
MASINT	measurement and signature intelligence
MI5	the UK Security Service
MI6	the UK Secret Intelligence Service
ODNI	Office of the Director of National Intelligence, US
ONI	Office of National Intelligence
OSINT	open-source intelligence
SIGINT	signals intelligence
UK	United Kingdom
US	United States

Collaborative and agile

Intelligence community collaboration insights from the United Kingdom and the United States

ISSN 2200-6648