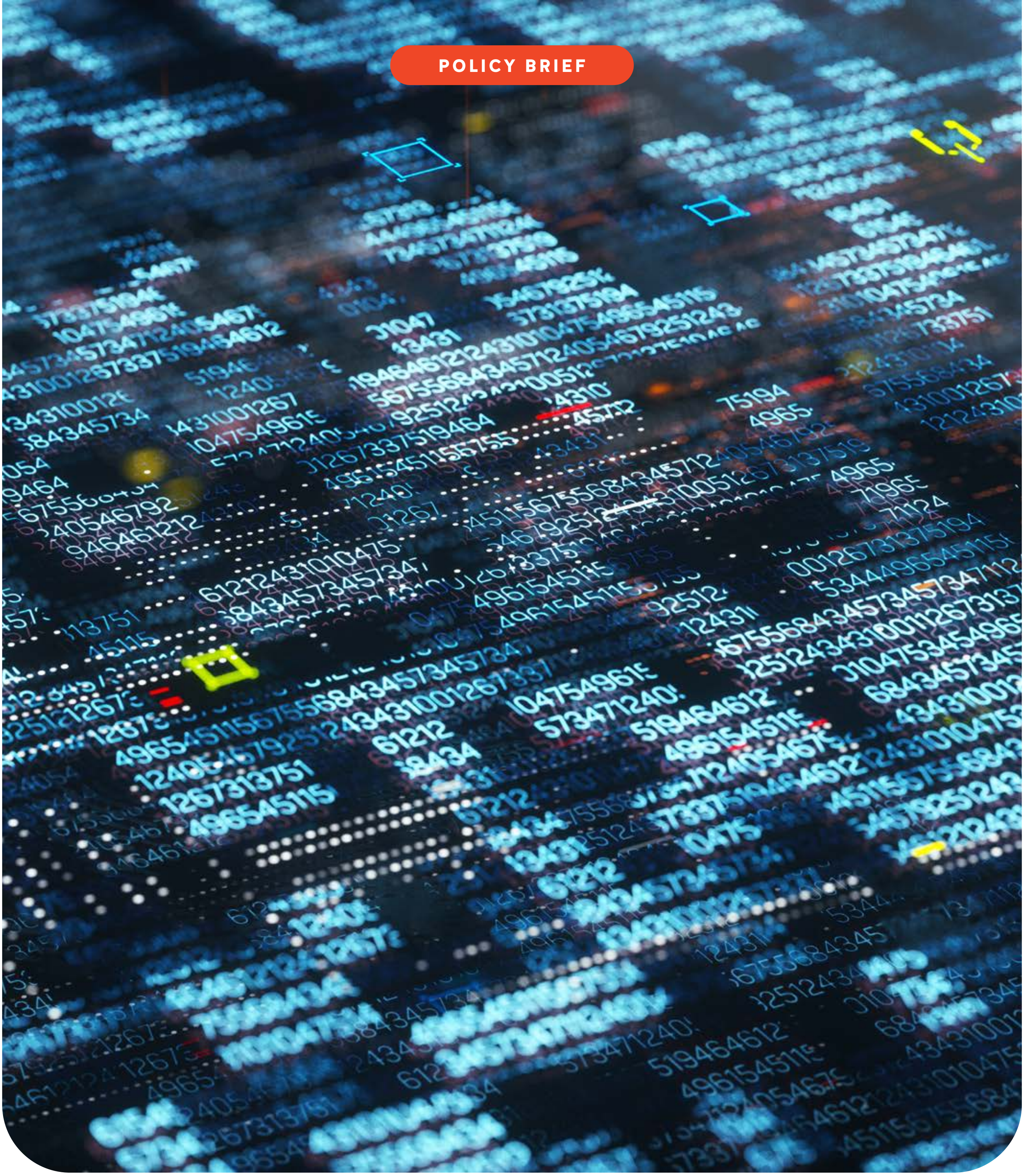
POLICY BRIEF



SECRECY, SOVEREIGNTY AND SHARING: HOW DATA AND EMERGING TECHNOLOGIES ARE TRANSFORMING INTELLIGENCE

DR MIAH HAMMOND-ERREY | FEBRUARY 2023

UNITED STATES
STUDIES CENTRE

Executive summary

- The Australian National Intelligence Community (NIC) – like all democratic intelligence communities – is experiencing a transformation brought on by digital disruption. Data abundance, digital connectivity and ubiquitous technology have formed a new 'big data landscape' which is the foundation for many data-driven emerging technologies, such as artificial intelligence (AI).

- Australian intelligence agencies and organisations are grounded in long-standing principles and practices, set out most recently in the Richardson Review.[1] Emerging technologies are challenging some of these foundational principles and practices of intelligence and impacting the organisations, activities and outcomes of intelligence. The big data landscape has implications for producing intelligence and possibly even for the objectives of the intelligence community.

- A key impact of technology and data is that very little is likely to remain secret forever. There is a shift in the role secrecy plays in intelligence work. Secrecy is still vital for protecting intelligence sources and methods, but much more is knowable or inferable about the world, and community expectations around transparency are changing. As some intelligence activities move increasingly into the public sphere, government must continue to rebalance the tension between secrecy and transparency, and raise policymaker awareness of the current long-standing deliberate and principled choices relevant to refining this balance.

- The evolution of the telecommunications industry has complicated user identification, shifting from point to point (i.e. landlines) to being data-driven and across many devices. This challenges the legislative requirement of the NIC to identify geographical jurisdiction and sovereignty. How do intelligence agencies compliantly identify 'Australian' people and data within the noise?

- Digital sharing is increasing within and between intelligence agencies but still requires improvement. Extant data-sharing issues remain with existing decision-makers, such as ministers, operational decision-makers and other government agencies, which could be improved using new technologies. Additionally, intelligence needs to be shared with new stakeholders, such as academia, industry and other government agencies, to optimise the opportunities – and counter the challenges – presented by data-driven technologies.

- The NIC needs to be more flexible in understanding data and culturally able to adapt to data-driven technologies. Improving digital information exchanges within the NIC and with decision-makers is critical, as is improving work culture and practices to embrace innovation and technology.

- The Australian Government should continue to explore new intelligence alliances, focused both around changing threat pictures and embracing new technologies. Deepening intelligence exchange with the United States and Five Eyes partners is critical, as is exploring new regional alliance partners.

- This policy brief draws on a larger research project that explored the impact of big data on intelligence production and national security decision-making in Australia. A unique data set included interviews with almost 50 NIC leaders and practitioners from each of the 10 agencies, who provided insight into the sometimes necessarily opaque processes and operations of intelligence agencies. More detail will be published in a book forthcoming in late 2023.

Introduction

Emerging technologies are redefining national security[2] and the way nations protect individual rights and freedoms.[3] The big data landscape – and the emerging technologies it drives – are challenging some of the fundamental principles and practices of intelligence, such as secrecy, sovereignty and citizenship, as well as stakeholder and decision-maker engagement. This policy brief considers the implications of data and data-driven emerging technologies for Australia's National Intelligence Community (NIC). It explains, for a broader policy audience, the role of the 10 agencies that form the NIC and provides insight into how emerging technologies impact intelligence agencies and their activities.

This policy brief draws on empirical research conducted at Deakin University, which involved interviews with almost 50 participants inside all the Australian NIC agencies. It focused on the unique impacts of big data and emerging technologies on intelligence and excluded discussion of broader technology issues felt by many industries, such as accessing the technology workforce. They are Australia's intelligence leaders and practitioners, and this policy brief draws on these previously unexplored perspectives. This unique empirical data set is explained in more detail at the end of this policy brief.

The 10 agencies of the NIC each perform specific intelligence collection and/or assessment functions and have different missions, purposes, cultures and levels of technological capability, and consequently different challenges. This policy brief provides a rare insight into the work of each agency as well as the challenges facing the community as a whole.

Emerging technologies are those which are still in development and/or the practical applications are largely unrealised.[4] They are technologies that have moved from the hypothetical realm (e.g. a space mirror that deflects the amount of solar radiation hitting the earth) to the research, development and prototyping stage (e.g. concentrated solar power farm). Collectively, emerging technologies prefigure disruptive changes to the economy, the nature of work, business, medicine, science and social interaction. Many emerging technologies are also dual-use[5] and, as a result, are more prevalent in industry and society, harder to track and pose more diverse and diffuse challenges. Data-driven emerging technologies are challenging the NIC across multiple domains and indicate that intelligence is – or should be – at a tipping point.

DATA-DRIVEN EMERGING TECHNOLOGIES ARE CHALLENGING AUSTRALIA'S NATIONAL INTELLIGENCE COMMUNITY ACROSS MULTIPLE DOMAINS AND INDICATE THAT INTELLIGENCE IS – OR SHOULD BE – AT A TIPPING POINT.

Emerging technologies have opened another vector of geopolitical competition, driving greater consideration and management of data and national data-driven capabilities. This is happening as the Australian NIC is implementing structural change and moving together as a national enterprise. In this increasingly contested geopolitical environment, Australia needs the best from our national security apparatus. Australia's choices on how to transform intelligence to meet these challenges will shape the next generation's security and defence posture.

The National Intelligence Community

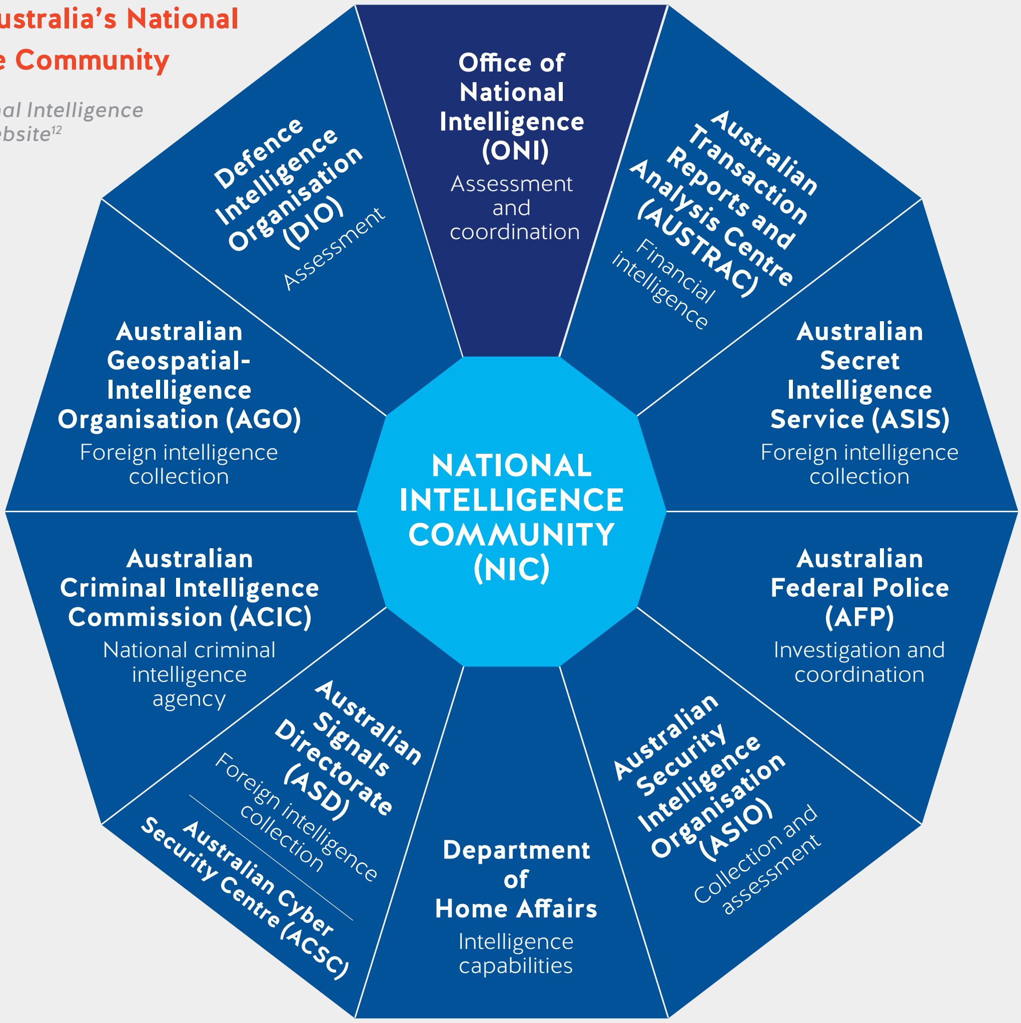
Ten agencies form the Australian Government's intelligence enterprise, working to collect, analyse and disseminate intelligence and advice in accordance with the nation's interests and national security priorities. Intelligence is information that has been collected, processed and analysed to support decision-making in relation to defence, foreign policy, national state affairs (such as diplomacy, trade and economics) and security.[6] It is 'knowledge vital for national survival.'[7] The basic purpose of intelligence is to 'improve the quality of decision-making by reducing ignorance, including reducing the vulnerability of the decision-maker to uncertainty.'[8]

Collectively, the Australian intelligence agencies are known as the National Intelligence Community (NIC). The NIC is a relatively new grouping of agencies, having expanded from six Australian Intelligence Agencies (AIC) to the 10 in the NIC after the 2017 Independent Intelligence Review.[9] The review found that whilst individual agencies were performing very well, a higher level of collective performance could be achieved by strengthening integration across Australia's national intelligence enterprise. Implementation of the most significant enterprise reform in the Australian intelligence world since the Hope Royal Commission[10] is slow and will require many years to truly assess.[11]

The main purpose of intelligence agencies is to protect national security, identify and assess threats and emergencies and support responses to them, as well as create and maintain a strategic advantage over potential adversaries and threats. Each national security agency has distinct missions and purposes which are critical to understanding the impact of technology on each agency. They perform specific intelligence collection and assessment functions and have different missions, purposes, cultures, and levels of technological capability. The agencies that form the NIC and their primary function are shown in Figure 1 below. The Office of National Intelligence (ONI) has an intelligence leadership and coordinating function.

Figure 1. Australia's National Intelligence Community

Source: National Intelligence Community website[12]


NATIONAL INTELLIGENCE COMMUNITY (NIC)
Office of National Intelligence (ONI)
Assessment and coordination
Australian Transaction Reports and Analysis Centre (AUSTRAC)
Financial intelligence
Australian Secret Intelligence Service (ASIS)
Foreign intelligence collection
Australian Federal Police (AFP)
Investigation and coordination
Australian Security Intelligence Organisation (ASIO)
Collection and assessment
Department of Home Affairs
Intelligence capabilities
Australian Signals Directorate (ASD)
Foreign intelligence collection
Australian Cyber Security Centre (ACSC)
Australian Criminal Intelligence Commission (ACIC)
National criminal intelligence agency
Australian Geospatial-Intelligence Organisation (AGO)
Foreign intelligence collection
Defence Intelligence Organisation (DIO)
Assessment

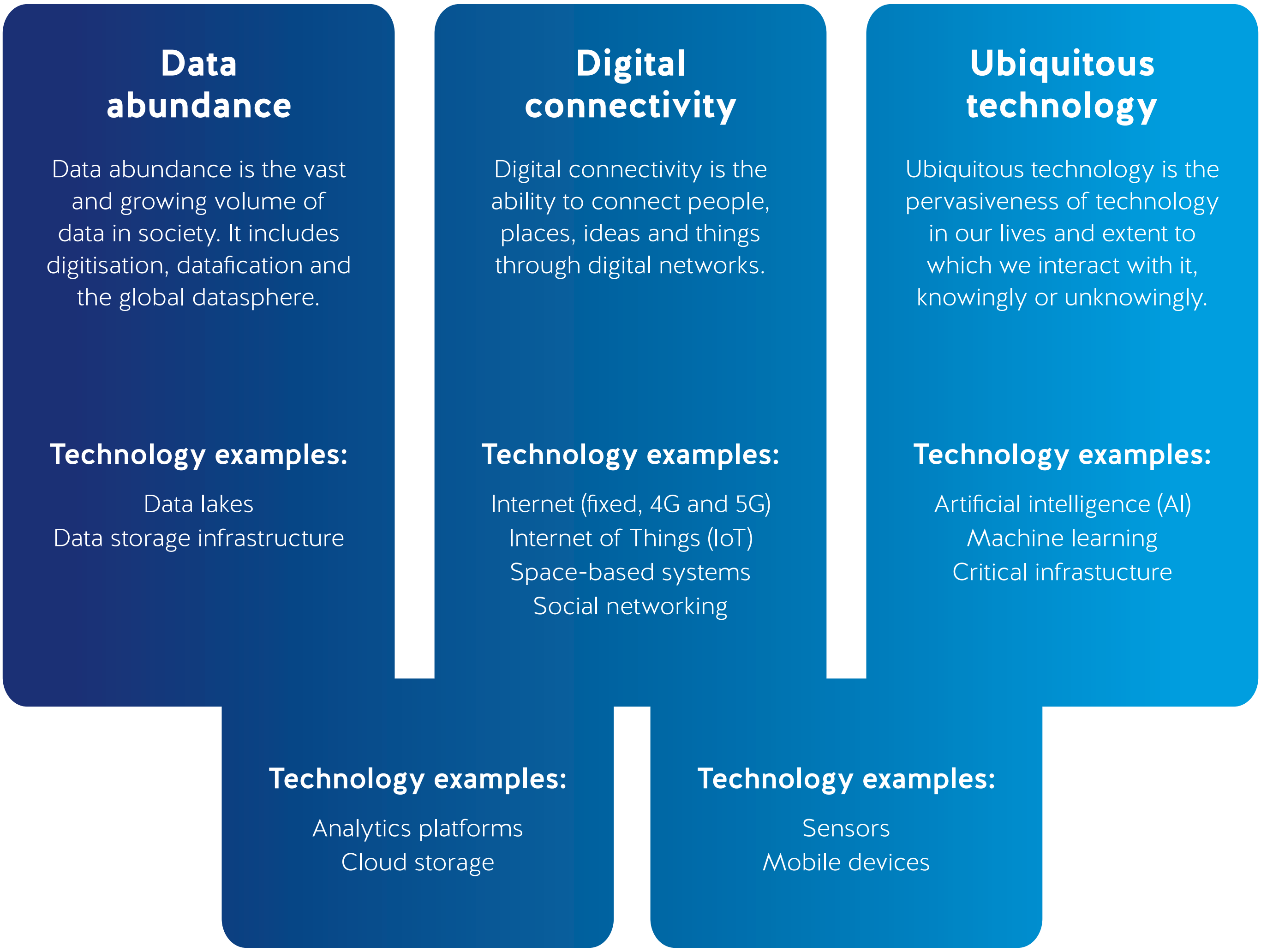
Emerging technologies

This policy brief explores emerging technologies fuelled by big data, such as artificial intelligence. The big data landscape, set out in *Big Data and National Security: A Guide for Australian Policy-makers*,[13] includes three key features with unique and significant implications for national security: data abundance, digital connectivity and ubiquitous technology (see Figure 2).[14] This landscape is the foundation for many emerging technologies impacting national security.

Interviewees indicated that many of the emerging technologies that are national security priorities are directly related to, or require big data.

The emerging technologies and advanced capabilities that intelligence leaders and practitioners described as the greatest national security interest include big data sets, AI, machine learning, synthetic biology, robotics, nanotechnologies, advanced materials, microwave space systems, telecommunications infrastructure (especially Internet of Things (IoT) and 5G), quantum computers and semiconductors. Big data-driven emerging technologies have and will continue to transform the global information landscape and national security operating environment.

Figure 2. Features of big data for intelligence



Data abundance

Data abundance is the vast and growing volume of data in society. It includes digitisation, datafication and the global datasphere.

Technology examples:

Data lakes
Data storage infrastructure

Digital connectivity

Digital connectivity is the ability to connect people, places, ideas and things through digital networks.

Technology examples:

Internet (fixed, 4G and 5G)
Internet of Things (IoT)
Space-based systems
Social networking

Ubiquitous technology

Ubiquitous technology is the pervasiveness of technology in our lives and extent to which we interact with it, knowingly or unknowingly.

Technology examples:

Artificial intelligence (AI)
Machine learning
Critical infrastucture

Technology examples:

Analytics platforms
Cloud storage

Technology examples:

Sensors
Mobile devices

Emerging technologies challenge fundamental intelligence principles and practices

Emerging technologies driven by the big data landscape – made up of data abundance, digital connectivity and ubiquitous technology – impact almost every aspect of the activities that intelligence agencies undertake. Some even suggest that technological transformation is challenging the intelligence community's 'raison d'être', requiring adaptation of the way agencies collect, process and analyse data as well as disseminate intelligence.[15] In Australia, each of the agencies in the NIC has a critical, distinct and enduring function. The way that emerging technologies impact their activities is specific to the legal framework, mission and purpose of each agency, as well as the kinds of intelligence work they do. Despite these different perspectives, they have a shared interest in improving their capability to collect, analyse and disseminate information.

Australia has made several deliberate, principled choices to manage and limit the powers and activities of the NIC agencies.[16] These principles have been chosen and considered over time and include, among others:

i. the separation of security intelligence and law enforcement;

ii. the separation of intelligence collection and assessment;

iii. the distinction between foreign intelligence and security intelligence;

iv. the distinction between operations that occur onshore and those that take place offshore; and

v. the distinction between Australians and non-Australians.[17]

These distinctions have been long discussed and, arguably, blurred – with some exceptions and technical assistance between function – but ultimately upheld.

Data-driven emerging technologies are impacting these fundamental intelligence principles, and the practices they underpin, in three distinct ways. Firstly, a shift in the practice of secrecy in intelligence work and intelligence activities, with an increasing social expectation for transparency and appetite for information. Secondly, the big data landscape challenges understandings of jurisdiction, affecting the distinction between operations that occur onshore and offshore, as well as challenging what constitutes 'Australian' and 'non-Australian' in the context of data. Thirdly, the big data landscape challenges existing NIC data-sharing arrangements, separation of intelligence activities and stakeholder engagement.

IN AUSTRALIA, EACH OF THE AGENCIES IN THE NATIONAL INTELLIGENCE COMMUNITY HAS A CRITICAL, DISTINCT AND ENDURING FUNCTION. THE WAY THAT EMERGING TECHNOLOGIES IMPACT THEIR ACTIVITIES IS SPECIFIC TO THE LEGAL FRAMEWORK, MISSION AND PURPOSE OF EACH AGENCY, AS WELL AS THE KINDS OF INTELLIGENCE WORK THEY DO.

Secrecy

Secrecy is a defining characteristic of intelligence and has long been considered, perhaps, the *most* integral component of intelligence activities and organisational culture. Much has already been made of the loss of secrecy and privacy in the digital era. Undoubtedly, emerging technologies make it more difficult for some activities to remain secret. There is extensive coverage of the impact of an abundance of data and open-source intelligence (OSINT) on intelligence agencies.[18] However, the significant nuance that is vital to this discussion too often seems to be lost in the public debate. The valuable role of OSINT does not render secret intelligence less valuable or significant. In fact, an argument can be made that it increases the premium on secret collection because so much is knowable in the public domain. Irrespective, this debate should not be framed as mutually exclusive. The key benefits come from combining covert intelligence with open-source information. As my former ASPI colleagues argued, “prioritisation of open sources doesn’t mean an end to specialist covert data collection.”[19] There are three distinct components of ‘secrecy’ within intelligence agencies and their activities, each are impacted differently by data-driven emerging technologies.

The first is what is often referred to as ‘secret’ or ‘covert’ collection. Depending on the specific agency or intelligence activity there are different aspects to facets of secrecy. It can refer to the fact that the collection itself is happening (in the case of a delayed notification search warrant), or that the capability to collect something which is itself secret (such as the precise capabilities of signals, technical and satellite intelligence collection), or both (that precise capabilities are directed at a specific target). A key impact of technology and data is that very little is likely to remain secret forever. Secrecy and transparency must continuously be rebalanced in a democratic state, and the gap between community expectation and intelligence capabilities must not be a gulf so far that it cannot be bridged. There have been recent moves to be more open, ranging from more addresses from agency heads, and more Australian Secret Intelligence Service (ASIS) staff being named publicly, to greater engagements with the private sector on innovation, science and research.[20]

The second component of secrecy concerns *how* information and data are collected and held by intelligence agencies. This is about compartmenting information into silos to reduce the risk of large breaches (or ‘unauthorised disclosures’). This is traditionally done either by segmenting – called ‘compartmenting’ – whole intelligence disciplines such as signals or human intelligence, conducted by different agencies and putting a specific compartment around small groups who are actively working on an issue. Big data directly challenges this approach to information collection, storage and analysis because insights are derived by analytics across data sets that are as large as possible. The NIC is looking to implement technology solutions to integrate, at pace, larger volumes of data from multiple disciplines and sources. It is understood a national cloud solution is currently in development,[21] although this is not without challenges. As the 2017 Independent Intelligence Review noted, the very nature of holding and connecting large digital data sets directly challenges the practice of compartmenting information and increases the risks and consequences of security breaches.[22]

SECRECY AND TRANSPARENCY MUST CONTINUOUSLY BE REBALANCED IN A DEMOCRATIC STATE AND THE GAP BETWEEN COMMUNITY EXPECTATION AND INTELLIGENCE CAPABILITIES MUST NOT BE A GULF SO FAR THAT IT CANNOT BE BRIDGED.

The third, and last, component of secrecy is preserving secrecy in an environment of increased communication, declassification of intelligence, and changing threat environments to share with a broader range of non-traditional stakeholders. Examples of this can be seen in the rapid declassification by the United States of intelligence in the days before the Russian invasion of Ukraine in 2022,[23] and the declassification of an intelligence community assessment of Russia’s activities in the 2016 US presidential election.[24]

The requirement for secrecy in intelligence activities and within the agencies that perform them are different. Secrecy requirements depend on the situation as well as different objectives, legislative frameworks and agency cultures. The type and temporality of the secrecy required varies. Here are a few examples of the kinds of secrecy requirements in Australian intelligence agencies:

- Investigation into **suspected terrorist activity** may have secrecy requirements bounded by the time of the investigation until action is taken. The majority of capabilities available to AFP, ACIC and ASIO to collect intelligence are set out specifically in legislation. The secrecy component is likely time-bound and limited in nature, irrespective of the technology used in intelligence collection or committing crimes.

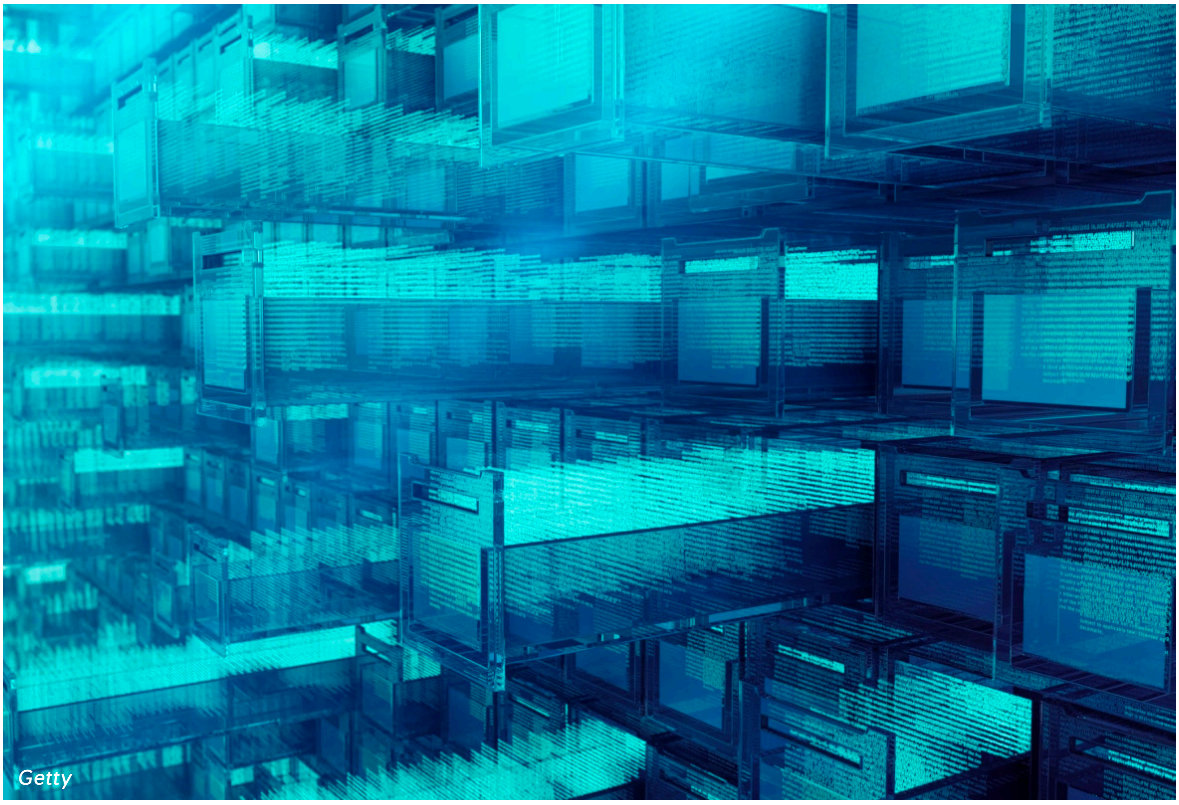
- Intelligence collection on adversary **defence capabilities**, such as foreign military technology programs or remote sensing capabilities in regional oceans, may have very few specific intelligence capabilities listed in the legislation. The secrecy component of these kinds of intelligence collection – and the capabilities used to collect it – have an enduring and critical secrecy requirement.
- **Human intelligence** collection offshore – and the data collection that guides it – could have enduring or limited temporal secrecy requirements, depending on the context. But the identity of agents recruited to provide intelligence on their country or organisation will have an enduring requirement for secrecy.

Policymaker discussions about secrecy need to appreciate these distinctions and consider what is and needs to be designated as secret. The increased politicisation of intelligence is visible in other democracies and it is not always clear that policymakers are aware of the significance of the aspects of secrecy mentioned above. This challenge has long existed, however data-driven technologies mean that the tensions between secrecy and transparency are – or will likely become – more public.

In addition to the impact on some fundamental principles, data-driven technologies are also impacting practices that have traditionally been central to the work of intelligence agencies. Secrecy is foremost among these. This means greater consideration is required now to ensure the protection of intelligence and intelligence capabilities (including collection methods, data and intelligence assessments), as well as transparency for accountability and communication to key stakeholders and declassification for non-government stakeholders.

Jurisdiction and sovereignty: What does 'Australian' data look like?

Geographical jurisdiction and nationality are critical for intelligence activities. In Western liberal democracies, foreign intelligence collection agencies are legislatively prohibited from collecting on their own citizens. In Australia, the legislative framework is based on fundamental intelli-



Getty

gence principles that make a distinction between Australians and non-Australians, and between operations that occur onshore and those that take place offshore.[25]

Australian intelligence agencies with a foreign collection mission are generally prohibited from collecting in Australia or on Australian citizens unless they have Ministerial approval.[26] The legislation – and well-accepted practice – for activities in Australia is that ASIO is responsible for security (domestic) intelligence and the agencies under the *Intelligence Services Act* are responsible for foreign intelligence collection.[27]

This requirement places significant importance on the distinction between what is Australian and non-Australian, whether that be people, places or data. The three features of the big data landscape challenge the practical reality of this distinction as they can obfuscate the geographical origin, transit and destination of communications, as well as the nationality of the user. This includes who owns data and infrastructure and where it resides, adding a layer of complexity for intelligence activities.

The sheer volume of information in society, and more specifically, who creates it, owns it and where it is based, obscures the originating or transit jurisdiction of data, both intentionally and unintentionally. Signals intelligence in the big data era is challenged by the need to distinguish nationality – and it is simply not always possible to make this distinction from small pieces of data alone, which can challenge compliance with existing national legislation. How does the intelligence community understand and provide assurance that the data it collects is done in a way that meets legislative requirements and maintains the trust of the government and therefore the public? This is becoming increasingly challenging due to the pace, volume and breadth of data sources used by the community, unclassified and classified.

In the intelligence business, nationality matters. To comply with their legislative framework, foreign intelligence agencies must distinguish 'Australian' data and entities from 'non-Australian' data and entities within the colossal data sphere. This is simply not always possible with contemporary digital communications, and new emerging technologies, such as artificial intelligence, will exacerbate this challenge. Nevertheless, nationality remains a critical distinction in intelligence collection and the desire to protect the privacy of Australians is closely connected to ideas of democracy and sovereignty. Furthermore, this can be complicated by the number of dual Australian nationals.

Challenges to NIC data sharing and decision-maker engagement

The contemporary infrastructure of the NIC – digital and physical – is challenged by the big data landscape and will be further fractured by emerging technologies such as AI. The current primary challenges are effective data sharing within NIC agencies and their stakeholders, and the ability to engage digitally with traditional and emerging decision-makers. Existing challenges to data sharing within the NIC remain extant and are exacerbated by big data and new technologies. Furthermore, there is limited whole-of-NIC technical oversight or technical support for existing oversight mechanisms. Engagement with decision-makers – from traditional policymakers to non-traditional stakeholders – requires structural and practical improvement.

THE SHEER VOLUME OF INFORMATION IN SOCIETY, AND MORE SPECIFICALLY, WHO CREATES IT, OWNS IT AND WHERE IT IS BASED, OBSCURES THE ORIGINATING OR TRANSIT JURISDICTION OF DATA, BOTH INTENTIONALLY AND UNINTENTIONALLY.

Internal data sharing

During interviews, NIC participants emphasised their ability – and often inability – to acquire and share digital information effectively between and with intelligence agencies, various arms of government, academia and industry and the community more broadly. Many intelligence processes are still manual, such as sharing printed paper copies, information on disks and emailing through to group inboxes. A consistent theme of this research was the challenge of sharing digital information and intelligence, let alone conducting big data analytics, between the former AIC and new NIC agencies. Whilst this is no doubt improving, intelligence leaders and practitioners describe the infrastructure as not set up to share or collaborate effectively and characterised many ICT systems as not fit-for-purpose across the whole community. Examples included the inability to communicate digitally across all agencies, such as email and video conferencing facilities.

Data sharing within the NIC is challenged by the differences in security classifications at which agencies operate. The original AIC agencies largely operate at Secret and Top Secret, whereas the additional 'NIC' four largely operate at the lower classification of Protected.[28] By design, it is difficult – and in some cases not possible – to transfer information between these systems and agencies with different security requirements. Each of these has different requirements in terms of varying access, IT robustness measures, storage length and protection measures, isolation from the internet and analytical capabilities. This means that analytical platforms and particularly some AI processes will require significant technical, cultural and security policy change to implement.

When intelligence gathering rests on degrees of data sharing, it becomes difficult to build genuine relationships and engage effectively with stakeholders. Participants indicated challenges in developing data-sharing practices domestically as well as internationally, and the difficulty of achieving whole-of-government and Five Eyes policy in this area.

Intelligence sharing with new stakeholders

Communication forms the link between intelligence collection, analysis and decision-making and is therefore a vital, but often under-considered, component of intelligence. The big data landscape significantly impacts the communication of intelligence and requires improved digital communication of intelligence to decision-makers. The *use* of intelligence by decision-makers is a critical part of the process: without use by decision-makers, intelligence would be redundant. In the intelligence world, it is usually referred to as dissemination. Communication of intelligence is often considered at the 'end' of the intelligence cycle when a completed analytical product or assessment is delivered to a decision-maker.

Often, in the case of tactical decision-making, the connections are relatively simple, such as identities, relationships and associations with other entities (people, places and things). In the case of strategic assessments, these might be significantly complex issues that need insight. An example might be how COVID-19 works and why certain vaccines might be better investments than others, the types of military capabilities an adversary is believed to have, vulnerabilities to foreign interference and espionage, or what organised crime trends Australia might face in the future.

DATA SHARING WITHIN THE NIC IS CHALLENGED BY THE DIFFERENCES IN SECURITY CLASSIFICATIONS AT WHICH AGENCIES OPERATE. THE ORIGINAL AIC AGENCIES LARGELY OPERATE AT SECRET AND TOP SECRET, WHEREAS THE ADDITIONAL 'NIC' FOUR LARGELY OPERATE AT THE LOWER CLASSIFICATION OF PROTECTED.

The challenge of sharing intelligence digitally with significant primary decision-makers was a common theme across interviews. Participants from all agencies talked about a variety of challenges present in sharing digital information in a timely fashion with their key stakeholders, including Ministers, internal decision-makers and other government agencies. Additionally, intelligence needs to be shared with new stakeholders. Australia's current strategic circumstances and increasing threat environment have created a greater need to share and engage with non-traditional partners, such as academia, industry and other government agencies.

Alliances and stakeholders

Nation state alliances and stakeholders are vital to intelligence sharing. Consideration of potential alliances and new stakeholders is an important and timely necessity. The current regional threat landscape combined with opportunities to transform intelligence capabilities using new technologies necessitate discussions about how to develop alliances for future readiness as well as expand to new stakeholders (whether they be decision-makers, the public or providers of data).

Alliances

Australia's closest intelligence partners – the United States, the United Kingdom and Canada – are also grappling with the ethical, operational and policy implications of big data for intelligence collection and analysis in open and democratic societies. Japan put policies in place in 2014 to classify secret information and is still yet to formalise a classification hierarchy on par with its peers.[29] The need for deeper intelligence cooperation with the United States, the United Kingdom and the Five Eyes community, as well as possible alliances with new countries such as Japan, are precipitated both by a shifting regional threat picture and emerging technologies, especially data, artificial intelligence, biotechnology, quantum and regional telecommunications.

Stakeholders

The big data landscape has created more diffuse vulnerabilities in sectors not previously associated with the intelligence community, such as the technology industry, universities, media, non-government organisations and state and territory governments. There is a need for increased engagement with non-traditional stakeholders on specific threats such as cyber-attack and espionage as well as seeking information from industry to help understand the threat landscape and identify offenders.

Since intelligence agencies increasingly need to mix internally held data with external data, they need to engage with new stakeholders. One example is to work with commercial entities to create indicators for analysis. Indicators – or signposts – 'are a list of observable events that one would expect to see if a postulated situation is developing,'[30] and are often used to understand intelligence problems such as economic reform, military modernisation, political instability, crime trends, illicit drug importations, weapons of mass destruction capabilities such as nuclear reactor development, and extremist radicalisation.

The use of indicators is common intelligence analysis practice which provides 'an objective baseline for tracking events or targets, indicators instil rigor into the analytic process and enhance the credibility of analytic judgments.'[31] Whilst some agencies have long used industry-based indicators, such as the Australian Transaction Reports and Analysis Centre for financial intelligence analysis, for some intelligence agencies it is relatively a new approach to intelligence. The big data landscape offers the possibility of large-scale data analysis to inform indicators. Examples include developing indicators of activities such as radicalisation and engaging with industry to identify activities or individuals involved. For example, large-scale data sets, such as purchase lists for weapons or chemicals, could be matched with intelligence holdings, ideally in real time.

Policy recommendations

1. Australia's contemporary intelligence infrastructure – digital and physical – is not match-fit for the present or the future. Australia needs an intelligence enterprise that can tackle the challenging missions it faces in the current and future environment. It is necessary to create a more agile intelligence infrastructure.

   - ONI should establish a task force to fast-track secure and simple digital exchange across the NIC. It is critical that this includes active collaboration with ASD, as the likely actioner for this effort and includes extensive consultation – and consensus – with the remaining NIC agencies. Without support from all agencies, cross-agency exchange will not succeed. In particular, the focus should be on improving digital information exchanges between NIC agencies (including between Top Secret and Protected) as well as with external stakeholders such as decision-makers, policy agencies, industry and increasingly direct to media and Australians.

   - To engage more effectively with existing and new stakeholders as well as share expenses, the NIC should develop digital infrastructure for multi-agency classified facilities that enable security-cleared staff to work from multiple locations, and enable cross-agency or stakeholder briefings and collaboration between larger groups. These facilities should also be able to increase international engagement. Learn from the best innovative and collaborative industry working practices, whilst preserving necessary physical security requirements.

   - It is necessary to create – at all classifications – multi-agency buildings that include more (and larger) meeting rooms, hot-desking capabilities, digital communications, and facilities in major cities, especially near transport hubs and where people want to live (to enable NIC employees to travel, move around and enable decision-makers secure access to information). ASD's REDSPICE initiative[32] is an excellent start, but NIC-wide approaches require systemic cultural change – toward collaboration and innovation – and leadership.

2. Alliances are critical for intelligence success, but little is known publicly about them. Dedicated and funded research is necessary to explore ways to improve intelligence exchange, technical capacity and burden sharing as well as intelligence diplomacy in the digital era.

   - The Australian Government should fund research to explore ways to improve intelligence alliances within the Five Eyes, and with other nations such as Japan and South Korea.

   - ONI should establish a unit focusing on digital experimentation, in conjunction with the National Security Science and Technology Centre to run pilot projects that address community-wide challenges on talent, processes and technologies identified by agencies. This agency should work with a recently proposed similar US agency,[33] if established.

   - Improve technical development and alignment in US and UK alliances and ensure integration between intelligence-led Five Eyes technical cooperation and Defence-led AUKUS advanced capability cooperation.

   - The United States, the United Kingdom and Australia should prioritise technical intelligence sharing and ensure integration with existing mechanisms, such as Five Eyes as well as AUKUS Pillar 2. Additionally, the key focus areas that are broader than the defence relationship, such as cyber and artificial intelligence, will likely require additional consideration.

DEDICATED AND FUNDED RESEARCH IS NECESSARY TO EXPLORE WAYS TO IMPROVE INTELLIGENCE EXCHANGE, TECHNICAL CAPACITY AND BURDEN SHARING AS WELL AS INTELLIGENCE DIPLOMACY IN THE DIGITAL ERA.

3. To respond to Australia's strategic circumstances, it is necessary to invest in, improve, and protect Australia's intelligence enterprise and the people behind it.

   - It is necessary to create more movement within the NIC and collaboration opportunities across government, think tanks, regulators, and technology companies to understand technology challenges and be equipped to counter them. Additionally, it is important to link agencies up with each other's information and data, and foster deeper understanding – and respect for – different agency missions, cultures and functions.

   - It is also important to improve 'whole-of-community' understanding, analysis and collaboration. Often, intelligence leaders and practitioners speak from experience in one or two agencies or intelligence disciplines. There appears to still be limited mobility and awareness about whole-of-community capabilities and challenges, as they are still compartmentalised in a way that does not encourage interdisciplinary collaboration, respect, appreciation and unity across agencies.

   - ONI should continue to implement and expand on recommendations from the Richardson Review to provide NIC-wide training on all NIC agencies, their background, cultures, mission and capabilities.

4. It is necessary to continue to rebalance the tension between secrecy and transparency. Governments need to preserve aspects of secrecy for security, while also protecting democratic principles (such as representative, responsible, transparent and accountable government and constitutional order).[34] It is necessary to delineate and communicate the significance of secrecy practices and trade-offs to policymakers, in the context of democratic transparency.

   - ANU's National Security College should include a module on the tensions between secrecy and transparency in National Security 23[35] – a parliamentarian training program recently announced by the Foreign Minister, Senator Penny Wong. Similar training should be included in state and territory legislative induction programs.

   - ONI should ensure the clear designation of capabilities for collection and analysis across all the NIC agencies. Ensure government has access to voices from all NIC agencies. Often specific agencies or intelligence disciplines are disproportionally reflected in discussion.

   - The Australian Government should ensure that secret intelligence capabilities are within the bounds of reasonable community expectations of intelligence services to avoid backlash where collection or capabilities are legal but do not reflect community expectations. Where this is not possible due to the nature of the threat, policymakers need to bridge the gap, explaining the threat to Australians, and increasing community awareness through engagement, working groups and forums.

   - The Australian Government should clarify existing powers and consider increased resourcing and powers for the Inspector-General of Intelligence and Security (IGIS), especially in relation to the new NIC agencies as well as the use of big data and emerging technologies. It should also consider the oversight role of the Parliamentary Joint Committee on Intelligence and Security (PJCIS).

   - ONI should lead NIC engagement and two-way dialogues on intelligence and national security to enable community attitudes to consider contemporary threats and ensure diverse perspectives and experiences are reflected within the intelligence enterprise.

TO RESPOND TO AUSTRALIA'S STRATEGIC CIRCUMSTANCES, IT IS NECESSARY TO INVEST IN, IMPROVE, AND PROTECT AUSTRALIA'S INTELLIGENCE ENTERPRISE AND THE PEOPLE BEHIND IT.

- As a part of the recently announced Strengthening Democracy Task Force,[36] the Australian Government should develop plans to increase trust in the institutions of democracy and ensure that the balance of secrecy and transparency is bipartisan and de-politicised.

5. Intelligence agencies need to build better relationships with government, industry and Australian citizens to respond to the changing digital landscape. NIC agencies have the opportunity to 'bake in' institutional and cultural approaches to build better relationships. Whilst this may seem self-evident, intelligence communities and public engagement can be inimical to each other and for some NIC members the concept remains revelatory.

   - Increasing agency capacity for two-way conversations with stakeholders may require a cultural change and specific training, especially for agencies for whom engagement outside the intelligence community is new. Additional areas for improvement include how intelligence agencies understand, relate to and access key decision-makers, getting the right people in the right rooms for collaboration and managing the flow of information and intelligence.
   - Intelligence agencies need to publicly recognise the value of diplomacy and advocate for further DFAT funding. Intelligence diplomacy has real potential in the current strategic environment, but not at the expense of DFAT, as many intelligence activities overseas rely on diplomatic facilities, relationships and capabilities.
   - ONI should establish an advisory board (drawn from industry and academia) to streamline access to technical expertise for the whole of the NIC as well as oversight bodies like the IGIS and PJCIS.

Conclusion

The big data landscape of data abundance, digital connectivity and ubiquitous technology is the foundation for many emerging technologies and is challenging fundamental principles and practices of intelligence. The foundational role of secrecy in intelligence is being challenged by a digital landscape which renders very little as secret forever. The digital landscape has expanded the potential for large-scale security breaches and requires new approaches to 'compartmenting' information to ensure security. The big data landscape has created more diffuse vulnerabilities in sectors not previously associated with the intelligence community and these require increased engagement with new stakeholders – a revelation for some NIC agencies.

THE BIG DATA LANDSCAPE HAS CREATED MORE DIFFUSE VULNERABILITIES IN SECTORS NOT PREVIOUSLY ASSOCIATED WITH THE INTELLIGENCE COMMUNITY AND THESE REQUIRE INCREASED ENGAGEMENT WITH NEW STAKEHOLDERS – A REVELATION FOR SOME NIC AGENCIES.

The big data landscape challenges 'foreign' and 'domestic' collection as it is simply no longer possible to identify nationality from data or location alone. The obfuscation of the originating or transit jurisdiction of data, combined with the need to distinguish nationality (of entities and data), requires deeper consideration and sharing with Australian people. This requires ongoing balancing between secrecy and transparency with particular attention to ensure bipartisan non-politicisation.

In addition, the big data landscape challenges both NIC data sharing and stakeholder engagement. The current, often manual, challenges faced by data sharing are exacerbated by new technologies and will continue to worsen. Furthermore, these will be compounded by the need for the NIC to engage with decision-makers from traditional policymakers as well as non-traditional stakeholders. This requires infrastructural as well as cultural change. Finally, a changing threat picture combined with the impacts of emerging technologies necessitates deeper consideration of intelligence alliances.

Method: Talking to Australia's National Intelligence Community

The author gained access to some of Australia's most highly regarded intelligence leaders and practitioners to provide insight and analysis into the challenges and opportunities of big data. Intelligence practitioners are well-positioned to provide insight into the impact of big data on the sometimes necessarily opaque processes and operations of the NIC. This policy brief draws on data collected as part of a larger research project that explores the impact of big data on intelligence production and national security decision-making in Australia.

The research was conducted at Deakin University between 2017 and 2021, and included human ethics approval. It involved semi-structured interviews with 47 senior and operational decision-makers as well as technologists working in Australia's national security and intelligence agencies. A selection of independent subject matter experts were interviewed, largely former heads of agencies or technical experts. Each of the NIC agencies participated in what is the first known piece of empirical research to cover the inner workings of all AIC and NIC agencies – as well as the oversight body, the Office of the Inspector-General for Intelligence Security – with between one and 10 members interviewed per agency.

Acknowledgements

The PhD research that underpins this policy brief, *Big Data and National Security: Impacts for Intelligence* was supervised by Dr Chad Whelan and Dr Diarmaid Harkin at Deakin University. Publications are available at https://miahhe.com. The PhD was supported by a National Security Big Data Scholarship from Data to Decisions Cooperative Research Centre (D2D CRC) and a University Postgraduate Research Scholarship from Deakin University. Additional support was also provided by D2D CRC in the form of an Applied Research and Collaboration Award (2017) and an Applied Research Grant (2019). Thank you to the many interviewees and peer reviewers of this policy brief.

ENDNOTES

1. Commonwealth of Australia, "Comprehensive Review of the Legal Framework of the National Intelligence Community" [also known as the Richardson review] (2020), 165. Available at: https://www.ag.gov.au/national-security/publications/report-comprehensive-review-legal-framework-national-intelligence-community.

2. David Rubin et al., "Harnessing Data for National Security," *SAIS Review* 34, no. 1 (2014).

3. There are many different conceptualisations of national security. The notion of values is highlighted as "the absence of threats to acquired values and subjectively, the absence of fear that such values will be attacked" by Arnold Wolfers, *Discord and Collaboration; Essays on International Politics* (Baltimore,: Johns Hopkins Press, 1962): 485. The "absence of threat" was subsequently refined as "a low probability of damage to acquired values" (David A. Baldwin, "The Concept of Security," *Review of International Studies* 23 (1997): 13).

4. Emerging technologies can be assessed by frameworks to assess their level of realisation, relative growth and impact. For example; (i) radical novelty, (ii) relatively fast growth, (iii) coherence, (iv) prominent impact, and (v) uncertainty and ambiguity (Daniele Rotolo, Diana Hicks, and Ben R. Martin, "What Is an Emerging Technology?," *Research Policy* 44, no. 10 (2015): 1827-1843).

5. This means that rapid technology innovations in the form of goods, software and technology that can be used for both civilian and military applications. It is difficult regulate one without foregoing the other, for more see Jonathan B. Tucker, *Innovation, Dual Use, and Security: Managing the Risks of Emerging Biological and Chemical Technologies* (Cambridge, Mass: The MIT Press, 2012).

6. Mark M. Lowenthal, *Intelligence: From Secrets to Policy*, 5th ed. (Los Angeles Thousand Oaks, California: SAGE/CQ Press, 2012); David Omand, *Securing the State* (New York: Columbia University Press, 2010); Sherman Kent, *Strategic Intelligence for American World Policy* (Princeton, New Jersey: Princeton University Press, 1966).

7. Sherman Kent, *Strategic Intelligence for American World Policy* (Princeton, New Jersey: Princeton University Press, 1966): vii.

8. David Omand, "Reflections on Intelligence Analysts and Policymakers," *International Journal of Intelligence and CounterIntelligence* 33, no. 3 (2020): 472.

9. The 2017 Independent Intelligence Review, commissioned in 2016 by then Prime Minister, the Hon Malcolm Turnbull MP, was largely focused on security environment and technology advancements and whether the intelligence community was working effectively and structured appropriately. It found that Australia's intelligence agencies are highly capable and held in high regard by their international partner agencies. The Review also found that as a result of transforming geopolitical, economic, societal and technological changes, the intelligence community will be faced with challenges that will intensify over the coming decade. See: Department of the Prime Minister and Cabinet Commonwealth of Australia, "2017 Independent Intelligence Review," (2017). Available at: https://www.pmc.gov.au/publications/report-2017-independent-intelligence-review.

10. The Royal Commission on Intelligence and Security, 1974–77 [also known as the Hope Royal Commission], assessed the history of Australian security and intelligence agencies. It also made recommendations about the role each agency has in serving Australia, their future and reviewed procedures as well as the functioning of ministerial control, direction and coordination. It delivered eight reports between 1976 and 1977, with many recommendations adopted by government. This included reforming and bureaucratising ASIO, along with many of the existing intelligence agencies. For more see National Archives of Australia, "Royal Commission on Intelligence and Security, 1974–77". Available at: https://www.naa.gov.au/explore-collection/intelligence-and-security/history-australian-intelligence-and-security/royal-commission-intelligence-and-security-1974-77; John C. Blaxland and Rhys Crawley, *The Secret Cold War. Volume III : the Official History of ASIO, 1976-1989* (Crows Nest, NSW: Allen & Unwin, 2016), 28.

11. Patrick F. Walsh, "Transforming the Australian Intelligence Community: Mapping Change, Impact and Challenges," *Intelligence and National Security* 36, no. 2 (2021): 243-259.

12. National Intelligence Community, "Who we are," Australian Government, NA. Available at: https://www.careersinintelligence.gov.au/who-we-are.

13. Miah Hammond-Errey, "Big Data and National Security: A Guide for Australian Policymakers," in *Lowy Institute Analysis* (Sydney, Australia: Lowy Institute, 2022).

14. The grouping of terms was first used by US intelligence leader Sue Gordon and in subsequent communication with the author she confirmed that to the best of her knowledge this grouping was her own construction. The same themes emerged in the larger research project as features of big data most relevant to intelligence. This research project offers empirical analysis to deepen understanding and define these terms.

15. Shay Hershkovitz, "How Tech Is Transforming the Intelligence Industry," *TechCrunch*, 11 August 2019. Available at: https://techcrunch.com/2019/08/10/how-tech-is-transforming-the-intelligence-industry/.

16. Commonwealth of Australia "Comprehensive Review," 165.

17. Commonwealth of Australia "Comprehensive Review," 165.

18. See for example Tess Horlings, "Dealing with Data: Coming to Grips with the Information Age in Intelligence Studies Journals," *Intelligence and National Security* ahead-of-print (2022); Sir David Omand, Jamie Bartlett, and Carl Miller, "#Intelligence," (London: Demos, 2012); and, Ardi Janjeva, Alexander Harris and Joe Byrne, "The Future of Open Source Intelligence for UK National Security," in *Occasional Paper* (London, UK: Royal United Services Institute for Defence and Security Studies, 2022).

19. Michael Shoebridge, John Coyne, and Rajiv Shah, "Collaborative and Agile. Intelligence Community Collaboration Insights from the United Kingdom and the United States," in *Special Report* (Australian Strategic Policy Institute 2021), 21.

20. Miah Hammond-Errey, "Securing the legal foundation for Australia's intelligence agencies," *The Interpreter*, 11 January 2021. Available at: https://www.lowyinstitute.org/the-interpreter/securing-legal-foundation-australia-s-intelligence-agencies.

21. James Riley, "Govt cloud scramble: The sovereign demands of Top Secret," *Innovation Aus*, 2 June 2022. Available at: https://www.innovationaus.com/govt-cloud-scramble-the-sovereign-demands-of-top-secret/.

22. Department of Premier and Cabinet Commonwealth of Australia, "2017 Independent Intelligence Review," 28. Available at: https://www.pmc.gov.au/sites/default/files/resource/download/2017-Independent-Intelligence-Review.pdf.

23. Amy Zegart, "Open Secrets: Ukraine and the Next Intelligence Revolution," *Foreign Affairs*, January 2023. Available at: https://www.foreignaffairs.com/world/open-secrets-ukraine-intelligence-revolution-amy-zegart.

24. US Senate Select Committee on Intelligence, "ODNI Statement on Declassified Intelligence Community Assessment of Russian Activities and Intentions in Recent U.S. Elections," 2017. Available at: https://www.intelligence.senate.gov/hearings/open-hearing-intelligence-communitys-assessment-russian-activities-and-intentions-2016-us.

25. Commonwealth of Australia "Comprehensive Review," 165.

26. The constraint on foreign intelligence collection is set out in the *Intelligence Services Act 2001 (Cth)* and the communication or dissemination of intelligence collected on Australians by foreign intelligence agencies is governed by Privacy Rules, which ASIS, ASD and AGO make available on their websites. It is possible to obtain Ministerial authorisation for some specific circumstances which are set out in the *Intelligence Services Act 2001 (Cth)* and Privacy Rules. Additionally, some agencies such as ASD have additional functions, such as cyber security collection in Australia. The blurring of boundaries between foreign and domestic intelligence functions and agencies is a complex and ongoing debate.

27. Commonwealth of Australia "Comprehensive Review".

28. Australian Government, "Sensitive and Classified Information," *Protective Security Policy Framework*, 28 September 2018. Available at: https://www.protectivesecurity.gov.au/publications-library/policy-8-sensitive-and-classified-information.

29. Michael M Bosack, "Looking back on Japan's secrets protection law," *Japan Times*, 19 December 2021. Available at: https://www.japantimes.co.jp/opinion/2021/12/19/commentary/japan-commentary/japan-

secrets-protection-law/; John Hemmings, ”How Might Japan Join the Five Eyes?,” *Centre for Strategic & International Studies*, 6 January 2023. Available at: https://www.csis.org/analysis/how-might-japan-join-five-eyes.

30. US Government, “A Tradecraft Primer: Structured Analytic Techniques for Improving Intelligence Analysis,” (2009): 12. Available at: https://www.stat.berkeley.edu/~aldous/157/Papers/Tradecraft%20Primer-apr09.pdf.

31. US Government, “A Tradecraft Primer”.

32. REDSPICE is a capability development program aimed at improving intelligence, offensive and defensive cyber, More available here: https://www.asd.gov.au/about/redspice

33. Special Competitive Studies Project, ”Intelligence in An Age of Data-Driven Competition,” *Special Competitive Studies Project* (October 2022): 16. Available at: https://www.scsp.ai/2022/10/scsps-intelligence-panel-releases-interim-panel-report/.

34. Parliamentary Education Office, ”Democracy,” 19 July 2022. Available at: https://peo.gov.au/understand-our-parliament/how-parliament-works/system-of-government/democracy/.

35. Dominic Giannini, ”National security school for politicians,” *Canberra Times*, 10 November 2022. Available at: https://www.canberratimes.com.au/story/7977259/national-security-school-for-politicians/.

36. The Hon Claire O’Neil MP, “Strengthening Democracy Taskforce”, Minister for Home Affairs, 2022. Available at: https://minister.homeaffairs.gov.au/ClareONeil/Documents/factsheet-strengthening%20-democracy-taskforce.pdf.

ABOUT THE AUTHOR

DR MIAH HAMMOND-ERREY

Director, Emerging Technology, United States Studies Centre

Dr Miah Hammond-Errey is the Director of the Emerging Technology Program at the United States Studies Centre at the University of Sydney.

Miah's work explores the intersections of emerging technologies and security. Previously she was a Senior Analyst at the Australian Strategic Policy Institute and has published across mainstream media and think tanks as well as in academic and military press.

Miah spent more than fifteen years leading tactical, operational, and strategic analysis and communications activities for the Australian Government with a focus on emerging trends, complex challenges, and national security threats. She has represented Australia overseas in Europe and Asia.

Miah's doctoral research examined the impact of big data on intelligence production and national security in Australia. This research was supported by a National Security Big Data Scholarship from Data 2 Decisions CRC and Deakin University Postgraduate Research Scholarship. This research was also awarded a D2D CRC Applied Research and Collaboration Award (2017) and an Applied Research Grant (2019). Miah also has a Master of National Security Policy (Advanced) with Honours from the National Security College at the Australian National University. Her dissertation presented an information influence and interference framework applied to Russian operations in Crimea, Ukraine and relating to the downing of MH17. Miah also has a Master of Criminology from the University of Sydney Law School and a Bachelor of Arts from the University of Sydney.

UNITED STATES
STUDIES CENTRE

The United States Studies Centre at the University of Sydney is a university-based research centre, dedicated to the rigorous analysis of American foreign policy, economics, politics and culture. The Centre is a national resource, that builds Australia's awareness of the dynamics shaping America – and critically – their implications for Australia.

UNITED STATES STUDIES CENTRE

Institute Building (H03), City Rd
The University of Sydney NSW 2006
Australia

+61 2 9351 7249
us-studies@sydney.edu.au

USSC.EDU.AU

THE UNIVERSITY OF
SYDNEY

AUS
USA
American
Australian
Association

Cover photo: Getty

This publication may be cited as:

Miah Hammond-Errey, "Secrecy, sovereignty and sharing: How data and emerging technologies are transforming intelligence," United States Studies Centre at the University of Sydney, February 2023.

Research conclusions are derived independently and authors represent their own view, not those of the United States Studies Centre. This research was peer-reviewed by both internal and external experts.