Australian National University | NATIONAL SECURITY COLLEGE

Adapting Australian intelligence to the information age

Ben Scott

OCCASIONAL PAPER DECEMBER 2023

About the author

Ben Scott is a Senior Advisor at the National Security College. He has more than 25 years' experience in diplomacy, think tanks, intelligence and international development. Ben has published widely on national security decision-making, international order, US grand strategy and competition with China, cyber strategy and intelligence.

About this paper

The ANU National Security College (NSC) is a joint initiative of The Australian National University and the Commonwealth Government. The NSC's Occasional Papers comprise peer-reviewed research and analysis concerning national security issues at the forefront of academic and policy inquiry. They are designed to stimulate public discourse and inform policy solutions.

NSC is independent in its activities, research and editorial judgment and does not take institutional positions on policy issues. Accordingly, the author is solely responsible for the views expressed in this publication, which should not be taken as reflecting the views of any government or organisation.

ANU National Security College
national.security.college@anu.edu.au

The Australian National University Canberra ACT 2600 Australia
www.anu.edu.au

CRICOS Provider No. 00120C
TEQSA Provider ID: PRV12002 (Australian University)

Contents

Executive Summary

Australia's intelligence institutions were created during the Cold War to obtain, protect, assess and disseminate secrets. After the Cold War, the digital revolution accelerated, creating an abundance of unclassified national security information. The information revolution is also creating a more complex information ecosystem, in which information cannot be neatly categorised as public or secret.

Australia must adapt its National Intelligence Community (NIC) to this new era. Following the lead of the United States, recent intelligence reforms have sought to overcome bureaucratic silos and improve integration. Although these reforms have targeted the counterproductive culture of secrecy, this culture remains a continuing obstacle to reform.

To create a more flexible NIC, Australia should redefine intelligence and its role. Intelligence is information that is useful for national security, regardless of its source. To rebalance the NIC's approach to open-source intelligence (OSINT), a dedicated OSINT organisation should be created. Because OSINT does not require secrecy, this reform would also disrupt the culture of secrecy. Done right, it would increase flexibility and adaptability across the NIC.

The Office of National Intelligence (ONI) should be charged with optimising the relationship between OSINT and secret intelligence. ONI should encourage synergies and complementarity so that OSINT improves the quality of secret intelligence, and vice versa. But ONI should also facilitate healthy competition. Comparisons between the utility of OSINT and secret intelligence will be difficult but necessary as Australia shapes its future intelligence effort.

Key points

- The digital information revolution is the most significant development in the history of intelligence, at least since the Second World War.
- To adapt, Australia's National Intelligence Community (NIC) must rebalance its work in favour of Open Source Intelligence (OSINT).
- Done right, this reform would result in a more flexible NIC producing intelligence – sourced both openly and secretly – that is more useful for the government.

Policy recommendations

- Clearly define intelligence as information that is useful for national security, regardless of its classification.
- Establish a dedicated OSINT agency as part of the NIC.
- Empower the Office of National Intelligence (ONI) to optimise the interaction between OSINT and secret intelligence.

Statecraft in the information age

"With the exception of weapons of mass destruction ... all the really vexing threats are to and through data."

Sue Gordon, Former US Principal Deputy Director of National Intelligence

As the digital information revolution has gained pace, information has become more central to statecraft. It is an increasingly valuable resource, a domain of competition, and at the heart of understanding and solving complex transnational problems.

The acceleration of Chinese industrial espionage and Russian digital disinformation were leading indicators of this trend. In 2015, the former was evocatively characterised as the "greatest transfer of wealth in history".[2] In the same year, China also stole personnel files relating to about 4 million current and former US federal employees.[3] In the 2016 US election, Moscow showed how its old tools of disinformation could be amplified in the digital age.

The centrality of information warfare was demonstrated again as Russia began its kinetic war against Ukraine in 2022. This time, Russia's opponents had the early advantage. Having completely revised its cyber doctrine, US Cyber Command sent its largest ever "hunt forward" deployment to Ukraine before the invasion.[4]

This blunted Russia's information operations, while the US and UK used intelligence to alert allies to Russian President Vladimir Putin's intention and "pre-bunk" Russian disinformation. The formation of a countervailing coalition was accelerated and Putin was wrong-footed. As one US official put it: "we were beating Putin's lie to the punch, and we know that by doing so we got inside his decision-making loop".[5] The cumulative effect arguably weakened Russia's military performance.[6]

1 Amy Zegart, *Spies, Lies and Algorithms* (Princeton University Press: 1 February 2022), p 255.

2 Josh Rogin, "NSA Chief: Cybercrime constitutes the "greatest transfer of wealth in history", *Foreign Policy*, 9 July 2012, accessed 10 November 2023, https://foreignpolicy.com/2012/07/09/nsa-chief-cybercrime-constitutes-the-greatest-transfer-of-wealth-in-history/

3 Brendan I. Koernerer, "Inside the Cyberattack That Shocked the US Government", *Wired*, 23 October 2016, accessed 10 November 2023, https://www.wired.com/2016/10/inside-cyberattack-shocked-us-government/

4 US Department of Defense Cyber National Mission Force Public Affairs, "Before the Invasion: Hunt Forward Operations in Ukraine", 28 November 2022, accessed 10 November 2023, https://www.cybercom.mil/Media/News/Article/3229136/before-the-invasion-hunt-forward-operations-in-ukraine/

5 Erin Banco, Garrett M. Graff, Lara Seligman, Nahal Toosi and Alexander Ward, "Something Was Badly Wrong': When Washington Realized Russia Was Actually Invading Ukraine" *Politico*, 24 February 2023, accessed 10 November 2023, https://www.politico.com/news/magazine/2023/02/24/russia-ukraine-war-oral-history-00083757

6 Ensign Nicholas J. Romanow, "The Promise and Danger of Declassifying Intelligence for Effect", *Proceedings*, Vol. 149/4/1,442, US Naval Institute, April 2023, accessed 10 November 2023, https://www.usni.org/magazines/proceedings/2023/april/promise-and-danger-declassifying-intelligence-effect

The information era

The information era is best understood as a consequence of the ongoing digital information revolution. Rapid take up of the internet in the mid-1990s was followed by the emergence of social media and Web 2.0 in the 2000s, the proliferation of smartphones in the 2010s and rapid advances in artificial intelligence in 2023.

The new information environment is typically defined in terms of the growing volume, variety and velocity of digital data. The volume is expected to double from 2022 to 2026.[7] This data also comes in an expanding variety — much of it is unstructured and opaque to those without specialist skills. However, some of it is instantaneously disseminated to a global audience. A single image can capture the public imagination and shift the international agenda.[8] Yet the sheer volume and variety of data can make it harder to assess value and veracity.

National security

National security in the information era will depend more on the ability of states to obtain, protect and optimally use this data. To compete effectively, Australia must be better at all these tasks than its adversaries are.

Australia's national security is also threatened by a widening array of transnational and transboundary issues. Climate change, economic de-risking, emerging technologies, public health, and violent extremism all intersect with geopolitics to create an environment of unprecedented complexity.[9] Comprehending this complexity is a new information and intelligence challenge.[10]

There is no simple model for statecraft in the information age. A coherent theory of the emerging information ecosystem is yet to be developed.[11] There are many paradoxes: data is both more abundant and more valuable, while the volume of data both reveals and obfuscates. There is much more to learn about the power of narratives — and disinformation — on human perception, cognition and action.[12] New technologies can be both clarifying and confusing. Advances in generative artificial intelligence could reset attempts to understand the emerging ecosystem.

The NIC will be central to Australian statecraft in the information age. Data is its core business. In September 2023 the government commissioned an independent review of the NIC, to be completed in 2024. The review should consider how to adapt the NIC to the information age. This falls within its terms of reference, specifically "how effectively the NIC serves, and is positioned to serve, national interests and the needs of Government" and "NIC preparedness in the event of regional crisis and conflict".

7 John Rydning "Worldwide IDC Global DataSphere Forecast, 2022–2026: Enterprise Organizations Driving Most of the Data Growth", Doc # US49018922, May 2022, accessed 10 November 2023, https://www.idc.com/getdoc.jsp?containerId=US49018922

8 Patrick Kingsley, "The death of Alan Kurdi: one year on, compassion towards refugees fades", Guardian 2 September 2016, accessed 10 November 2023, https://www.theguardian.com/world/2016/sep/01/alan-kurdi-death-one-year-on-compassion-towards-refugees-fades

9 Josh Kerbel, "It's true, the world always has been complex — but not like this", *The Hill* (9 May 2022), accessed 10 November 2023, https://thehill.com/opinion/national-security/3478119-its-true-the-world-always-has-been-complex-but-not-like-this/

10 This is clearly recognised in the 2023 US National Intelligence Strategy, accessed 10 November 2023, https://www.dni.gov/index.php/newsroom/reports-publications/reports-publications-2023/3713-2023-national-intelligence-strategy

11 Alicia Wanless Monday, "There Is No Getting Ahead of Disinformation Without Moving Past It" *Lawfare*, 8 May 2023, accessed 10 November 2023, https://www.lawfaremedia.org/article/there-is-no-getting-ahead-of-disinformation-without-moving-past-it

12 See, Josh Baughman and Peter Singer, "China's social-media attacks are part of a larger 'cognitive warfare' campaign" *Defense One*, 17 October 2023, accessed 10 November 2023, https://www.defenseone.com/ideas/2023/10/chinas-social-media-attacks-are-part-larger-cognitive-warfare-campaign/391255/

Secret intelligence in the information age

"Strategic competition is no longer just about the volume of data, it is about who can collect, access, exploit, and gain actionable insight the fastest, as they will have the decision and intelligence advantage."

US Intelligence Community Data Strategy 2023-2025

The West's response to Russia's invasion of Ukraine has been hailed as creating a "new model for how intelligence can support geopolitical goals."[13] There is much to learn from the conflict in Ukraine (see "Lessons from Ukraine", below) including about what intelligence must deliver. This includes open-source and secret intelligence, as well as intelligence that can be quickly operationalised. The production of intelligence must keep pace with accelerated decision making and information competition. Intelligence does not just enable national security decisions, it can shape narratives and influence perceptions. But the new model for intelligence is far from developed. This section focuses on how the information revolution is, and should be, changing the business of secret intelligence.

The rise of OSINT

The growing abundance of publicly available information (PAI) is the most obvious feature of the new information environment.

The discipline — or, more accurately, disciplines — of OSINT have proved themselves in Ukraine by collectively piercing the fog of war more thoroughly than in any previous conflict.

Many have argued that OSINT is therefore replacing, or at least reducing the need for, secret intelligence. Mark Lowenthal, a foremost expert on US intelligence, estimates that during the Cold War "80 per cent of the information the US required was secret and 20 per cent was open".[14] In the information era there is, according to Carmen Medina and Zachary Tyson Brown, a "declining market for secrets".[15]

This framing is too simple. Less of the national security information Australia needs may be secret, but it does not follow that Australia needs less secret intelligence. Indeed, the growing volume of data may have increased the quantity of potentially useful secrets. More importantly, the value of secret intelligence lies in its quality, rather than its quantity.

13 Stephanie Carvin, "Deterrence, Disruption and Declassification: Intelligence in the Ukraine Conflict" *Centre for International Governance Innovation*, 2 May 2022, accessed 10 November 2023, https://www.cigionline.org/articles/deterrence-disruption-and-declassification-intelligence-in-the-ukraine-conflict/

14 Marc Lowenthal, *Intelligence: From Secrets to Policy* (United States, CQ Press, 2017: 7th edition) p 107.

15 Carmen Medina and Zachery Tyson Brown, "The Declining Market for Secrets: U.S. Spy Agencies Must Adapt to an Open-Source World", *Foreign Affairs* 9 March 2021

Australia still needs quality secret intelligence. It will become more important for Australia to understand the secret intentions and capabilities of its competitors and adversaries. The challenge will be to ensure that scarce classified intelligence resources are tightly focussed on valuable secret information.

The information revolution is transforming every step of the processes through which governments seek, create and use secret intelligence.

Collection

- Collectors of secret intelligence must focus their scarce resources on information that is not otherwise obtainable. To identify the most valuable secrets, collectors must therefore stay abreast of relevant publicly available information.
- The quality of intelligence collection depends on the gap between collection capabilities and the target's awareness of those capabilities. But that gap is narrowing as public awareness of intelligence grows. The shocking 7 October 2023 Hamas attacks in Israel demonstrated the ability of even the most surveilled targets to deceive sophisticated collectors.
- Intelligence collectors are increasingly challenged by advances in commercially available encryption and the use — by counter-intelligence services — of an array of information technologies, including "smart city" surveillance and big-data processing.[16] Human intelligence officers need ever more sophisticated digital cover stories.

Protection

- The volume and variety of information that can affect national security, and therefore must be protected, is expanding. This includes more commercial, scientific and personal information.[17] Massive thefts of the personal data of Australians have underscored the volume and variety of data that must be protected.
- Protecting information is harder in the digital age. A single point of failure can cause a massive breach. A decade after the Snowden leaks, the 2023 "discord leaks" demonstrated the persistence of this vulnerability.[18]

Analysis and assessment

- Analysts and assessors turn raw intelligence into useful information. Access to secrets should, in theory, enable a small pool of security-cleared analysts to produce more useful information than larger groups of open-source analysts can. But the number of issues for which this is true is shrinking because of both the growth of open-source data and the range of national security issues.
- It is sometimes argued that intelligence organisations cannot contribute much to solving problems such as "the will to fight" or climate change because they are "mysteries" as opposed "puzzles".[19] But governments will still ask the NIC to help address these problems, which are better described as complex, as distinct from complicated.[20]

16 Paul Symon, "Foreign espionage: An Australian perspective", Speech: Sydney: 9 May 2022, , accessed 10 November 2023, https://www.lowyinstitute.org/publications/foreign-espionage-australian-perspective

17 Office of the Director of National Intelligence, The National Counterintelligence and Security Center, *Safeguarding Science: An Outreach Initiative for Protecting Research and Innovation in Emerging Technologies*, accessed 10 November 2023, https://www.dni.gov/index.php/safeguarding-science; https://www.washingtonpost.com/national-security/china-harvests-masses-of-data-on-western-targets-documents-show/2021/12/31/3981ce9c-538e-11ec-8927-c396fa861a71_story.html

18 Devlin Barret and Shane Harris, "Leak suspect indicted on new counts of mishandling classified material" *Washington Post*, 16 June 2023, accessed 10 November 2023, https://www.washingtonpost.com/discord-leaks/

19 Gregory F. Treverton, "Risks and Riddles" *Smithsonian Magazine*, June 2007, accessed 10 November 2023, https://www.smithsonianmag.com/history/risks-and-riddles-154744750/

20 On complicated versus complex, see Josh Kerbel "National Security Language Is Stuck in the Cold War" *Slate*, 5 October 2021, accessed 10 November 2023, https://slate.com/technology/2021/10/national-security-language-cold-war-sloppy-thinking.html. For an example of the continuing government need for intelligence agencies to address complex problems: Daniel Hurst, "Anthony Albanese to order intelligence chief to examine security threats posed by climate crisis" *Guardian* 22 June 2022, accessed 10 November 2023, https://www.theguardian.com/environment/2022/jun/22/anthony-albanese-to-order-intelligence-chief-to-examine-security-threats-posed-by-climate-crisis

Dissemination and operationalisation

- To effectively disseminate secret intelligence to policy and decision makers, intelligence organisations must know what these customers already know and think. This, in turn, requires understanding the constant flow of unmediated and unverified information these customers are receiving.
- The age-old trade-off between preserving intelligence and using it is shifting. The conflict in Ukraine demonstrated the growing benefits of disseminating intelligence faster and wider. It has shown how OSINT can be used to mask insights derived from secret intelligence. At the same time, the risks of exposing sources and methods has been reduced by greater public knowledge of methods (if not sources).
- Protecting privately held data requires intelligence organisations to share more information derived from classified intelligence with the private sector.[21]

Old categories, new environment

In the new information era, the Cold War categories of "openly sourced" and "secret" information are increasingly inadequate for understanding the national security value of data.

The public availability of "openly sourced" information varies greatly. Less than one per cent of the internet is indexed by Google. Cyber space is increasingly fragmented by the use of firewalls, security protocols and digital encryption by individuals, corporations and states. According to a report from the US Council on Foreign Relations, an open, reliable, and secure global network … is unlikely ever to be realized … the internet is less free, more fragmented, and less secure".[22]

The extraordinary development of commercial intelligence illustrates this mismatch between existing classification categories and the national security value of information. Commercial capabilities increasingly match or exceed those of nation states.[23] Private sector geospatial intelligence (GEOINT) has led the way, but increasingly sophisticated signals intelligence capabilities are also on the market.[24] Although corporations lack the legal authorities of intelligence organisations they are, by the same token, less constrained by privacy legislation.

Private data brokers aggregate and correlate greater masses of personal data than Western intelligence organisations can. A recently released US intelligence community report on the topic notes that: "the proliferation of digital dust created by individuals in their daily lives … includes information on nearly everyone that is of a type and level of sensitivity that historically could have been obtained, if at all, only through targeted … collection".[25]

21 Office of the Director of National Intelligence, The National Counterintelligence and Security Center, *Safeguarding Science: An Outreach Initiative for Protecting Research and Innovation in Emerging Technologies*, accessed 10 November 2023, https://www.dni.gov/index.php/safeguarding-science

22 Nathaniel Fick and Jami Miscik, Confronting Reality in Cyberspace, Council on Foreign Relations, July 2022, accessed 10 November 2023, https://www.cfr.org/task-force-report/confronting-reality-in-cyberspace

23 Mark Mazzetti and Ronen Bergman, "A Front Company and a Fake Identity: How the U.S. Came to Use Spyware It Was Trying to Kill" *New York Times,* 10 April 2023, accessed 10 November 2023, https://www.nytimes.com/2023/04/02/us/politics/nso-contract-us-spy.html

24 Cortney Weinbaum, Steven Berner, and Bruce McClintock, "SIGINT for Anyone: The Growing Availability of Signals Intelligence in the Public Domain", RAND Corporation: 2017, accessed 10 November 2023, https://www.rand.org/pubs/perspectives/PE273.html

25 Office of the Director of National Intelligence Senior Advisory Group Panel on Commercially Available Information, *Report to the Director of National Intelligence*, 27 January 2022, accessed 10 November 2023, https://www.dni.gov/files/documents/FOIA/DF-2023-00146-Senior-Advisory-Group-Panel-on-CAI.pdf

A more adaptable NIC

It is too early to try to rebuild the NIC around the still-evolving information environment. But the NIC must become more flexible; for example, in the application of national classifications. The government has asked the 2024 independent intelligence review "whether the use of the classification system by the NIC achieves the right balance between protecting sensitive information and providing decision making advantages to policy makers and operators". Although it is difficult to imagine a more functional taxonomy, it seems clear that optimally balancing protection and useability will require more flexible application of existing classifications.[26]

The downgrade, declassification and dissemination of intelligence by the US and UK before and during Russia's invasion of Ukraine has been rightly hailed as a success. But it is also true that much of this intelligence was — almost by definition — over-classified.[27]

The initial mechanism for reclassification was reactive and rudimentary. According to US National Security Advisor Jake Sullivan, "we … would … send to [the intelligence community] in classified form the things that we wanted to be able to say, they would tell us what could be declassified, and what couldn't".[28]

Although a major restructure would be premature, the NIC must significantly boost its use and production of OSINT. Because OSINT is not derived from secrets, it should not be understood simply as another type of "INT" but as a different set of disciplines. Amy Zegart correctly characterises OSINT and classified intelligence as different "ecosystems" with differing advantages and disadvantages: "one ecosystem is more open, diffuse, diverse and fast-moving. The other is more closed, tailored, trained and slower moving".[29] The NIC needs to take advantage of both intelligence "ecosystems" and optimise the interaction between them.

26 Australia's protective security classification system was recently, and wisely, simplified. See Chris Taylor, "Classifications and clearances are the bricks and mortar of national security", 20 June 2023, accessed 10 November 2023, https://www.aspistrategist.org.au/classifications-and-clearances-are-the-bricks-and-mortar-of-national-security/

27 Chris Rasmussen "Avoiding the Secrecy Trap in Open Source Intelligence" *Cipher Brief,* 21 March 2023, accessed 10 November 2023, https://www.thecipherbrief.com/column_article/avoiding-the-secrecy-trap-in-open-source-intelligence

28 Erin Banco, Garrett M. Graff, Lara Seligman, Nahal Toosi and Alexander Ward, "Something Was Badly Wrong': When Washington Realized Russia Was Actually Invading Ukraine" *Politico*, 24 February 2023, accessed 10 November 2023, https://www.politico.com/news/magazine/2023/02/24/russia-ukraine-war-oral-history-00083757

29 Amy Zegart, *Spies, Lies and Algorithms* (Princeton University Press: 1 February 2022) p 238.

Lessons from Ukraine

The war in Ukraine has shown how liberal democracies can and should use intelligence in the information era. A few lessons stand out:

- The discipline of OSINT has proved itself. The contrast between Moscow's murky 2014 incursion into Ukraine and its 2022 invasion could not be sharper.[30]
- Secret intelligence remains valuable. Rapid advances in OSINT have not rendered it irrelevant. Washington and London used high-grade secret intelligence to forewarn of the Russian invasion, going against the weight of public expert commentary.
- Intelligence can play a crucial role in information competition. The US and UK downgraded, declassified and disseminated intelligence at an unprecedented scale and speed. They used more-easily disseminated OSINT to mask insights derived from secret intelligence.[31]
- Secret intelligence is not a crystal ball. Western intelligence agencies incorrectly forecast a quick Russian victory. This followed their failure to anticipate the speed of the Taliban's takeover of Afghanistan six months earlier.

30 "How spies, soldiers and the public should use open-source intelligence" *Economist*, 18 January 2023, accessed 10 November 2023, https://www.economist.com/leaders/2023/01/18/how-spies-soldiers-and-the-public-should-use-open-source-intelligence

31 Andrew Hammond, "Ukraine & the Alliance with NATO's Assistant Secretary General for Intelligence David Cattler" *Spycast* (Podcast) Episode 585, 3 May 2023, accessed 10 November 2023, https://thecyberwire.com/podcasts/spycast/585/notes

Intelligence reform and the secrecy problem

To adapt to the information age, the NIC must become more flexible, but Australia's intelligence organisations were not built for flexibility. They were established in and for the Cold War, with secrecy in their DNA.

Institutionalising secrecy

Because intelligence has such a long history, it is easy to forget the extent to which Five Eyes intelligence institutions are products of the Cold War. During that contest, the Five Eyes countries built a formidable multi-layered bureaucracy to obtain, protect and exploit secrets. This included secrecy legislation, secure infrastructure, customised information technology, compartmented information management and invasive vetting of personnel.

Obviously, secrecy is essential to secret intelligence, but it is also an impediment to flexibility. Secret bureaucracy is less exposed to competition, public oversight and accountability, while secret institutions tend to generate a "culture" of excessive secrecy. That culture has been blamed for the frequent over-classification of intelligence, a perennial problem that has been the subject of numerous reviews, but very little effective reform.[32]

It has also been identified as an obstacle to necessary intelligence sharing among allies, with policy makers and even between intelligence organisations in the same country.

This culture of secrecy is also frequently invoked as the main obstacle to making more use of PAI and OSINT.[33] Laboratory testing shows that intelligence analysts ascribe more value to secret intelligence than to identical OSINT,[34] and there is strong anecdotal evidence of this bias. In the words of Robert Cardillo, former Director of the National Geospatial-Intelligence Agency (NGA), says "we used to sprinkle open source or unprotected data at the end, right? We'd finish, you know, our highly classified report, and then we'd take a look around, read a paper, watch TV, you know, and add something".[35] According to Carmen Medina, Central Intelligence Agency (CIA) Deputy Director of Intelligence, and Zachery Tyson Brown, former Defence Intelligence Agency analyst, US intelligence organisations expect analysts to justify the expense of intelligence collection "by maximising the amount of highly classified material in their papers and presentations".[36]

The culture of secrecy can be understood as a product of skewed incentive structures — an exacerbated form of typical public service risk aversion. Rigid security clearance processes have produced a workforce that is more homogenous and thus more vulnerable to group think.[37]

32 Henry Sokolski, "Over-classification: How Bad Is It, What's the Fix?" (Non-proliferation Policy Education Centre: Occasional Paper, 28 March 2023, accessed 10 November 2023, https://npolicy.org/over-classification-how-bad-is-it-whats-the-fix-occasional-paper-2303/

33 Michael Morell, "Kristin Wood on the intelligence value of open source data — "Intelligence Matters" Podcast: CBS News: 8 March 2023, accessed 10 November 2023, https://www.cbsnews.com/news/kristin-wood-on-the-intelligence-value-of-open-source-data-intelligence-matters/

34 Tore Pedersen & Pia Therese Jansen, "Seduced by secrecy – perplexed by complexity: effects of secret vs open-source on intelligence credibility and analytic confidence", *Intelligence and National Security*, (34:6, 881-898, 13 June 2019)

35 Center for Strategic and International Studies, "Sparking a Revolution in Open Source Intelligence" Online Event, 3 December 2021, accessed 10 November 2023, https://csis-website-prod.s3.amazonaws.com/s3fs-public/event/211203_Harding_Sparking_Revolution.pdf?VersionId=h3lTl.MiLb2BKvQ.pyrYHM8.NYQpeHp1

36 Carmen Medina and Zachery Tyson Brown, "The Declining Market for Secrets: U.S. Spy Agencies Must Adapt to an Open-Source World", *Foreign Affairs* 9 March 2021

37 Matthew Connelly and Patricia Irvin, "How Secrecy Limits Diversity" *Foreign Affairs* 12 May 2023, accessed 10 November 2023, https://www.foreignaffairs.com/united-states/how-secrecy-limits-diversity

The culture of secrecy often manifests in the view that intelligence is valuable because it is secret, rather than secret because it is valuable. So information is classified to make it appear more valuable. Psychological factors are probably relevant here: the "endowment effect" describes the human tendency to attach more value to items we own simply because they belong to us, while the "sunk cost fallacy" describes our tendency to persist with an endeavour we are already invested in.[38]

Because different institutional arrangements produce different cultures, it is reasonable to assume that Australian intelligence analysts are less likely to privilege classified information. Unlike the CIA, neither Australia's ONI nor its Defence Intelligence Organisation (DIO) are responsible for intelligence collection. The 2004 Inquiry into Australian Intelligence Services found that "Office of National Assessments (ONA) product draws heavily on published or open source material, it is the single largest source of material for ONA reporting".[39] More recently, the Director General of National Intelligence specifically rejected the argument that secret intelligence is inherently more valuable than OSINT.[40]

Nevertheless, the NIC is structured to privilege classified information, so it is unrealistic to assume that it has entirely escaped the culture of secrecy.

Reforming intelligence

The intelligence bureaucracies established during the Cold War have undergone several rounds of reform. These have grappled with different manifestations of the secrecy problem. Australian intelligence reform has been shaped by a series of domestic reviews and greatly influenced by developments in the US.

In the mid-1970s, both Australia and the US launched commissions to deal with issues of oversight and accountability. Following the terror attacks of 11 September 2001 and the 2003 US-led invasion of Iraq, a further round of US reform focussed on the lack of sharing within the intelligence community, as well as the United States Intelligence Community's unsatisfactory use of OSINT.

The Australian reviews are: the 1991 Review of the Intelligence Community Post-Cold War; the 1995 Commission of Inquiry into the Australian Secret Intelligence Services; the 2004 Inquiry into the Australian intelligence services ("the Flood review"); the 2011 Independent Review of the Intelligence Community ("the Cornall-Black review"); the 2017 Independent Intelligence Review ("the L'Estrange-Merchant review"); and the 2021 Comprehensive Review of the Legal Framework Governing the National Intelligence Community (the "Richardson review").

Intelligence integration

Washington's main response to inadequate sharing within the intelligence community has been increased "intelligence integration".[41] The 2004 *Intelligence Reform and Terrorism Prevention Act* (IRTPA) created a new Director of National Intelligence (DNI), charged with leading and integrating the work of the US intelligence community.

But intelligence integration almost foundered on the rocks of institutional politics.[42] The core problem for "vertical integration", as envisaged by the new DNI construct, has been that it cuts across the horizontal lines of responsibility, in which the US Intelligence Community's (then) 17 agencies and elements were already embedded. Congressional haggling over the IRTPA led to the Military Intelligence Program budget being carved out of the National Intelligence Program. The first three DNIs struggled to assert their authority and served fewer than two years each. Only during the tenure of Jim Clapper, DNI from 2010-17, was substantial progress made on intelligence integration.

Clapper's success encouraged Australia to follow suit. The central goal of the 2017 L'Estrange-Merchant review was creating "an even higher level of collective performance through strengthen-

38 See Daniel Kahneman, *Thinking, Fast and Slow* (London: Penguin Books: 2011) p. 289

39 Australian Government, *Report of the Inquiry into Australian Intelligence Services*, (July 2004) p. 104

40 Rory Medcalf, Andrew Shearer and Mike Burgess, "Australia's intelligence leaders in conversation", National Security Podcast: 15 June 2023, accessed 10 November 2023, https://www.oni.gov.au/role-intelligence

41 US Government, National Commission on Terrorist Attacks. *The 9/11 Commission report: final report of the National Commission on Terrorist Attacks upon the United States* (United States: Norton, 2004), 401

42 Michael Allen, *Blinking Red: Crisis and Compromise in American Intelligence after 9/11* (University of Nebraska Press: 2013)

ing integration across Australia's national intelligence enterprise."[43] The Australian Intelligence Community (AIC) was rebadged as the National Intelligence Community (NIC) and expanded. The Office of National Assessments (ONA) was subsumed into a larger Office of National Intelligence (ONI) (see "The National Intelligence Community", below).

Australian intelligence integration has, however, been limited by the same structural tensions. The key implementing legislation, the *Office of National Intelligence Act,* is a bureaucratic compromise that falls short of the goals described in the L'Estrange-Merchant review. While the 2017 review recommended a Director General (DG) would be able to "direct the coordination of the NIC", the *ONI Act* describes the DG's role as merely "guiding the direction of the national intelligence community… to ensure…appropriate integration of matters relating to the national intelligence community".[44] Intelligence integration has been further weakened by "stubbornly entrenched portfolio and agency-based capability development and funding", often summarised as the "return of the portfolio".[45]

OSINT reform

The lodestar for intelligence reform since 9/11 has been adapting intelligence institutions to the demands of counter-terrorism, rather than the new information environment. Nevertheless, the counter terrorism challenge was often characterised as informational: "finding a needle in the haystack". Drawing on longstanding criticism of the US Intelligence Community (USIC)'s inadequate exploitation of open source data, in July 2004 the US 9/11 Commission recommended the creation of an OSINT agency.

In the same month, the Flood review recommended transferring the Open Source Unit (OSU) in the Department of Foreign Affairs and Trade (DFAT) to ONI's predecessor, the ONA. This was done. Although Australia's OSINT capability remains in ONI, it has evolved significantly over time. (See *Open Source Intelligence options*, below).

The US approach to OSINT remains unsettled. This reflects both continued bureaucratic competition and dissatisfaction with the current production of OSINT. The proposed OSINT agency was overtaken by the establishment of the Office of the Director of National Intelligence (ODNI). In 2005, the DNI announced the creation of a DNI Open Source Centre. Although this subsumed the CIA's Foreign Broadcast Intelligence Service, it remained housed in the CIA. In 2015, OSC effectively returned to the CIA and was renamed the Open Source Enterprise (OSE). But in 2021, Congress mandated the DNI to contract an independent study of OSINT and in particular "whether to establish a new agency as an element of the intelligence community dedicated to open-source intelligence".[46]

43 Commonwealth of Australia, Department of the Prime Minister and Cabinet, *Report of the 2017 Independent Intelligence Review* (Australia: Australian Government 2017) p 5.

44 Commonwealth of Australia, *Office of National Intelligence Act* (NO. 155, 2018) s 8.

45 Chris Taylor, "Australia's next intelligence review must learn from the past" *ASPI Strategist*, 29 June 2023, accessed 10 November 2023, https://www.aspistrategist.org.au/australias-next-intelligence-review-must-learn-from-the-past/

46 US Congress, *Intelligence Authorization Act For Fiscal Year 2021* s 623 1 F, accessed 10 November 2023, https://www.congress.gov/116/plaws/publ260/PLAW-116publ260.pdf
See also: US Senate Select Committee on Intelligence, *Explanatory Statement*, accessed 10 November 2023, https://www.intelligence.senate.gov/publications/joint-explanatory-statement-accompany-division-w-consolidated-appropriations-act-2021

More OSINT and stronger integration

The digital information revolution is the most consequential development in the history of intelligence, at least since the Second World War. The development of satellite imagery in the 1950s was momentous — and produced new intelligence organisations — but did not disrupt the fundamental model of secret intelligence.

The adaptability of secret intelligence organisations to this new environment is constrained by an entrenched culture of secrecy. The US intelligence community's data strategy frankly acknowledges that "to date, we have not significantly prioritised data as a strategic and operational Intelligence Community (IC) asset" and that improving capabilities requires "changes to historical, system-centric paradigms, years of legacy practices … (and) culture.[47]

Rather than reinventing the wheel, future intelligence reform should build on earlier efforts to both boost OSINT capabilities and strengthen integration. These two lines of effort should go hand-in-hand. The NIC must enhance its OSINT capabilities to ensure that it is gaining the most from publicly available information. But providing government with the best intelligence will also require integrating OSINT and secret intelligence. At the same time, boosting OSINT can help weaken the culture of secrecy and so encourage more flexibility in the NIC.

These reforms require an updated concept of intelligence.

47 Office of the Director of National Intelligence, *IC Data Strategy 2023-2025*, p 2, accessed 10 November 2023, https://www.dni.gov/files/ODNI/documents/IC-Data-Strategy-2023-2025.pdf#page=2

The National Intelligence Community

What came to be known as the Australian Intelligence Community (AIC) was formed from six intelligence agencies, of which five were established after the Second World War. In 1947, Australia's wartime signals intelligence capability was formed into the Defence Signals Bureau. The Australian Security Intelligence Organisation and the Australian Secret Intelligence Service were formed in 1949 and 1952 respectively. To assess intelligence, Australia established the Joint Intelligence Organisation in 1969 and the Office of National Assessments in 1978. In 2000, the Defence Imagery and Geospatial Organisation was added. Several of these organisations have changed their names over time.

On the recommendation of the 2017 Independent Intelligence review, the AIC was expanded and renamed. The "National Intelligence Community" (NIC) includes the following 10 agencies, or their intelligence components:

- Office of National Intelligence (ONI)
- Australian Security Intelligence Organisation (ASIO)
- Australian Secret Intelligence Service (ASIS)
- Australian Signals Directorate (ASD)
- Australian Geospatial-Intelligence Organisation (AGO)
- Defence Intelligence Organisation (DIO)
- Australian Criminal Intelligence Commission (ACIC)
- Australian Federal Police (AFP)
- Australian Transaction Reports and Analysis Centre (AUSTRAC)
- Department of Home Affairs

Defining intelligence

Australia should clarify the role of intelligence in its statecraft and in the government's wider adaptation to the new information environment. A tighter definition of intelligence would enable more intelligence integration. Defining intelligence in terms of the usefulness of information, rather than its secrecy, would help counter the culture of secrecy and better enable OSINT.

The missing link

Intelligence is undefined in Australian legislation. Like its Five Eyes partners, Australia has put organisations whose existence was once secret on a legislative footing. The Richardson review notes that "in 1979 … the legislative framework for the intelligence community totalled 86 pages. In August 2018, the framework stood at approximately 2,300 pages".[48] Although the *ASIO Act* was passed in 1956, the functions of ASIS were not defined in legislation until 2001, in the *Intelligence Services Act* (ISA).

The ISA specifies that "intelligence information" is intelligence obtained (or produced) by ASIS, AGO, ASD or DIO. In the case of ASIS that is "intelligence about the capabilities, intentions or activities of people or organisations outside Australia".[49] The *ONI Act* does not define intelligence, but describes one of ONI's functions as being to "assemble, correlate and analyse information relating to international matters that are of political, strategic or economic significance to Australia, including domestic aspects relating to such matters".[50]

The Richardson review notes that there is "no consensus in academic literature on the definition of intelligence".[51] There are several possible reasons for this. Although many sophisticated definitions have been proposed (see "Definitions of Intelligence, below), the more complex these are, the more debatable and less workable they become.

For practical purposes, governments (and intelligence organisations) have generally assumed that intelligence is whatever intelligence organisations do. This includes a spectrum of activities — from intelligence collection and analysis to covert operations. to covert operations. Australian and US efforts at intelligence integration have thus focussed on a wide range of activities whose common thread is secrecy. ONI lists seven: "collection, assessments, partnerships, intelligence diplomacy, disruption and effects, investigations and advice".[52] Secrecy has advantages and disadvantages, but is not a useful organising concept for intelligence, especially in the information age.

Enabling integration

A tighter definition of intelligence would enable more intelligence integration. Australian and US intelligence integration has been hampered by continuing bureaucratic divisions. The problem is not just "turf battles", there is an inherent tension between vertical integration and the horizontal lines of responsibility to Ministers. Logically, intelligence organisations also seek autonomy in their areas of specialisation. The opaque and confusing language of the *ONI Act* reflects the difficulty of resolving these tensions.

48 Australian Government, Attorney Generals Department, *Report of the Comprehensive Review of the Legal Framework of the National Intelligence Community*, 4 December 2020, p 154.

49 Commonwealth of Australia, *Intelligence Services Act 2001* s.6

50 Commonwealth of Australia, *Office of National Intelligence Act* (NO. 155, 2018) s 7(1)

51 Australian Government, Attorney Generals Department, *Report of the Comprehensive Review of the Legal Framework of the National Intelligence Community*, 4 December 2020, p. 154

52 Office of National Intelligence, Intelligence, "Intelligence: How our work protects and advances Australia's interests" , accessed 10 November 2023, https://www.oni.gov.au/about/our-work/intelligence

Rather than seeking to integrate the disparate activities of intelligence organisations, ONI should be charged with integrating intelligence information. Not everything that intelligence organisations do is intelligence; the collection, analysis, assessment, dissemination and protection of national security information are activities that add value to intelligence but are not, in themselves, "intelligence".

Advice is not intelligence. Australia's longstanding demarcation between intelligence and policy advice should be reinforced as the role of intelligence in statecraft grows.[53] Intelligence organisations cannot be seen to be tailoring intelligence to suit decision maker preferences or using their informational advantage to advance particular policy objectives.

Covert operational activities are not intelligence. That does not make them less important. Activities, such as "disruption and effects", are playing a growing role in intensifying in competition short of war (or in the "grey zone"). They should therefore be clearly distinguished from intelligence.[54] In particular, actions intended to shape the information environment should, insofar as possible, be separated from efforts to understand it (see "Information Operations" below).

Integrating intelligence information would be a more conceptually coherent mission for ONI, but also one that would require focusing resources as the volume, variety and velocity of information grows.

Enabling OSINT

The core purpose of intelligence is to inform, regardless of the source of information. A clearly source-agnostic definition of intelligence would help counter the culture of secrecy and enable OSINT. It is true that Australian legislation does not define intelligence as secret information and ONI's Director General uses a definition that does not depend on sources.[55] But this is relatively recent. Reflecting prevailing wisdom of the time, the Flood review defined intelligence as "covertly obtained information".[56] The culture of secrecy, and the associated assumption that intelligence is secret, is longstanding and pervasive.

Yet intelligence cannot simply be a synonym for information. Intelligence is information that is useful. Indeed, the value of intelligence depends on its usefulness. Raw data, regardless of classification, is rarely useful. Typically, the more processed information is, the more useful it becomes. Collection, protection, analysis and dissemination all add value.

53 The Richardson review correctly underscored the importance of reinforcing this distinction. Australian Government, Attorney Generals Department, *Report of the Comprehensive Review of the Legal Framework of the National Intelligence Community*, 4 December 2020, 3.4

54 See Will Stoltz, "A Regrettable Necessity: The Future of Australian Covert Action" *Occasional Paper* (ANU National Security College, May 2022, accessed 10 November 2023, https://nsc.crawford.anu.edu.au/publication/20309/regrettable-necessity-future-australian-covert-action

55 Rory Medcalf, Andrew Shearer and Mike Burgess, "Australia's intelligence leaders in conversation", National Security Podcast: 15 June 2023, accessed 10 November 2023, https://www.oni.gov.au/role-intelligence

56 Australian Government, *Report of the Inquiry into Australian Intelligence Services*, July 2004, p. 5

Intelligence should be defined as information that is useful for national security. This is more succinct and flexible than, for example, the formulation used in the *ONI Act*. Information that is clearly unrelated to national security is not intelligence, but there is probably no need to define "national security" narrowly.

Intelligence can be useful in a variety of ways: for context, sense making, policy making, decision making, or operationally. The usefulness of information depends on both its inherent qualities (accuracy, importance, insightfulness) and its functional utility (relevance to government priorities, the speed and ease with which it can be disseminated, discussed and acted upon). The simple concept of intelligence as useful information therefore provides a good framework for weighing the costs and benefits of different forms of intelligence.

Statecraft, intelligence and public policy in the information age

The government should also define the role of intelligence within its much wider efforts to adapt to the information era. This effort extends well beyond intelligence. The government has appointed new stand alone Freedom of Information and Privacy Commissioners, released draft combatting misinformation and disinformation legislation, commissioned and responded to a major review of the 1988 *Privacy Act,* and released a new Cyber Security Strategy. It has also drafted a national strategy for identity resilience and digital ID legislation. The Australian Electoral Commission is conducting a social media literacy campaign, while the Australian Competition and Consumer Commission is investigating the data brokering industry.

Definitions of Intelligence

ONI Director General Andrew Shearer defines intelligence as "nothing more than information that can provide decision makers with advance warning of threats to our national security or our national prosperity, but also of opportunities that we might face as a nation".

The Richardson review concluded that "intelligence, as used in government" can be a process, a product or an organisation.[57] This accords with Mark Lowenthal's definition of intelligence as "the process by which specific types of information important to national security are requested, collected, analysed, and provided to policy makers; the products of that process; the safeguarding of these processes and this information by counterintelligence activities; and the carrying out of operations as requested by lawful authorities".[58]

The L'Estrange-Merchant review defined intelligence as "value-adding contextual insights and actionable information, thereby reducing the cost and uncertainty in which government decisions are ultimately made and where appropriate contributing to the implementation". The Cornall-Black review defined it as "information that enables you to protect your interests or to maintain a valuable advantage in advancing your interests over those posing threats to them".

Justice Hope approved the US Rockefeller Commission's definition of intelligence as being "information gathered for policy makers which illuminates the range of choices available to them and enables them to exercise judgement".

57 Australian Government, Attorney Generals Department, *Report of the Comprehensive Review of the Legal Framework of the National Intelligence Community* (4 December 2020) p. 154

58 Marc Lowenthal, *Intelligence: From Secrets to Policy* (United States, CQ Press, 2017: 7th edition) p 1.

Information Operations

Democratic governments seek to shape the information environment with tools ranging from public diplomacy to propaganda through to what the UK National Cyber Force describes as "cognitive effects".[59] The dissemination of intelligence for effect, sometimes described as "intelligence diplomacy", is another tool.

Because democracies have a strong strategic interest in the integrity of the international information order, their information operations should be better governed and far more calibrated than those of authoritarian states. That is why, in the US and UK, offensive cyber action is undertaken by distinct organisations, US Cyber Command and the UK National Cyber Force respectively.

59 UK National Cyber Force, *Responsible Cyber Power in Practice* (March 2023) https://www.gchq.gov.uk/files/NCF_Responsible_Cyber_Power_In_Practice.pdf

Open-source intelligence options

"With the largest war in Europe since World War II occurring, intelligence capabilities were in high demand. This did not, however, diminish the frustration of walking out of the SCIF, turning on our phones, and gaining access to more (and more relevant) open-source content than we had at our workstations."[60]

Five Eyes intelligence organisations have been grappling with the question of how to make better use of open sources, and produce better OSINT, for several decades.

But what is OSINT? The term is often used expansively to encompass any information that is not classified. But OSINT is not a synonym for open-source data or searching the web. Rather, it is useful national security information produced from unclassified data, whether that data is freely or commercially available. For many decades, OSINT was produced chiefly by monitoring, translating and summarising the international press. But as the volume, variety and velocity of data has grown, so too has the complexity of producing accurate and valuable OSINT, and the need for specialist skills to do so.

Australia's OSINT capability is housed in ONI. It was transferred to ONA from DFAT on the recommendation of the Flood review. The Flood review's rationale is contained in one paragraph:

"ONA product draws heavily on published or open-source material. It is the single largest source of material for ONA reporting. Given its significance … the Open Source Unit … should be relocated to ONA. This would allow ONA to effect greater integration of open-source material into assessment, ensuring that analysts are at less risk of losing sight of the substantial source material in the open domain. It would also enable ONA to manage open-source collection within the broader construct of the intelligence burden-sharing arrangements, which is how the US views it."[61]

With the benefit of hindsight, this rationale appears less compelling. Given that open-source material was already the largest source of material for ONA reporting, it is unclear why analysts were in danger of losing sight of it. More importantly, the Flood review did not appear to consider the disadvantages of housing an OSINT capability within a secret organisation, including the prohibitive requirement for staff to maintain a top secret security clearance. Another reason for the move was to align Australia's approach to OSINT with America's, which it broadly did.

60 Brian Cheng, Scott Fisher and Jason C. Morgan, "Find It, Vet It, Share It: The US Government's Open-Source Intelligence Problem and How to Fix It." *Modern War Institute*, 24 March 2023, accessed 10 November 2023, https://mwi.usma.edu/find-it-vet-it-share-it-the-us-governments-open-source-intelligence-problem-and-how-to-fix-it/

61 Australian Government, *Report of the Inquiry into Australian Intelligence Services*, July 2004, p. 104

But the USIC's approach to OSINT continued shifting and, in Washington, dissatisfaction with the status quo is growing once again.[62] Dissatisfaction with the CIA's OSE has reportedly led to more US agencies creating their own OSINT units.[63] This dissatisfaction lends support to Amy Zegart's argument that "as long as open-source intelligence remains embedded in secret agencies that value clandestine information above all, it will languish".[64]

The wider US debate about the future of OSINT has generated the following three baskets of options:

- Enhancing OSINT capabilities within USIC elements.
- Establishing a dedicated OSINT organisation within the USIC.
- Obtaining more OSINT from outside the USIC.

A blue ribbon panel on the future of intelligence, convened by the US Center for Strategic and International Studies (CSIS) and chaired by Avril Haines (before she was nominated to her current post as DNI) settled on a narrower range of options, but could not agree on which to recommend:[65]

- Moving the Open Source Enterprise (OSE) from the CIA to the State Department.
- Moving the OSE (back) to ODNI.
- Establishing an independent open-source intelligence agency.

The following three Australian options are compared below:

- Enhancing NIC OSINT capabilities.
- A separate OSINT organisation within the NIC.
- A separate OSINT organisation outside the NIC.

62 Michael Morell, "Kristin Wood on the intelligence value of open source data — "Intelligence Matters", Podcast: CBS News: 8 March 2023, accessed 10 November 2023, https://www.cbsnews.com/news/kristin-wood-on-the-intelligence-value-of-open-source-data-intelligence-matters/

63 Peter Mattis, "How to Spy on China" *Foreign Affairs* 28 April 2023

64 Amy Zegart, "Open Secrets: Ukraine and the Next Intelligence Revolution" *Foreign Affairs* January/February 2023

65 Brian Katz, "Maintaining the Intelligence Edge Reimagining and Reinventing Intelligence through Innovation, A Report of the CSIS Technology and Intelligence Task Force", January 2021, accessed 10 November 2023, p. 20 https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/210113_Intelligence_Edge.pdf

Option 1: enhancing the NIC's OSINT capabilities

ONI's approach to OSINT has evolved significantly since the OSU was transferred from DFAT to ONA. Initially, it focussed on producing OSINT as a relatively discrete product line. Reports usually classified "For Official Use Only" were disseminated within government and to international partners. Over time, ONA addressed the tension between open-source work and a classified operating system. To bypass bottlenecks in the security clearance process, more staff without top secret security clearances were recruited to undertake open-source work, and separately accommodated until higher level clearances could be processed.

The Open Source Intelligence Branch (OSIB), as it is now known, still produces discrete OSINT reports but its production of OSINT has become more tightly focussed on – and integrated with – other, classified, intelligence missions. OSIB remains at the heart of NIC OSINT efforts. In addition to reporting, it provides leadership, coordination and a centre of tradecraft excellence.

There is a strong argument for continuing to strengthen OSINT skills within the ONI and across the NIC. All Australian intelligence reviews for the last 20 years have called for more OSINT training and technology. In the information age everyone — and especially intelligence officers — will need stronger information skills. In the words of Robert Cardillo, the former Director of the NGA, "open source is everyone's job".[66] Cardillo, a member of the CSIS panel, has since clarified that he opposed all three options identified earlier (on page 22).

Whether the NIC and ONI can keep evolving fast enough to keep pace with the rapidly evolving unclassified information environment is impossible to assess from the outside. Still, the success of ONI's innovations do not prove that there are no better arrangements for meeting the growing challenge of absorbing, structuring, triaging, analysing and verifying large, disparate and fast-moving data sets.

Much will depend on technology. Those within the system are generally far more optimistic about technical solutions than those who have recently left it.[67]

OSE/CIA Director Randy Nixon has forthrightly and commendably defended OSE's objectives and performance.[68] He has described how OSE is developing ChatGPT-style AI for use across the US intelligence community.[69] It is unclear whether this meets the call from CIA veteran Emily Harding for the CIA to develop its own cloud-based artificial intelligence tool. According to Harding, the USIC must accept the consequent risk of operating in the unclassified space. The alternative is to "pursue a fool's errand in trying to move the entire internet onto the high side, then search it with antiquated tools".[70] Harding identifies the culture of secrecy as the main impediment.

A detailed UK report on the future of OSINT is hopeful for the ability of a new Cabinet Office platform to "help analysts process information across both publicly available source and internal government reporting". It argues that "a centralised OSINT agency" is therefore "currently not the optimal course of action for the UK national security community".[71]

66 Center for Strategic and International Studies, "Sparking a Revolution in Open Source Intelligence" (Online Event, 3 December 2021, accessed 10 November 2023, https://csis-website-prod.s3.amazonaws.com/s3fs-public/event/211203_Harding_Sparking_Revolution.pdf?VersionId=h3lTl.MiLb2BKvQ.pyrYHM8.NYQpeHp1

67 For example, Bob Ashley and Neil Wiley, "How the Intelligence Community Can Get Better at Open Source Intel", Defense One, 16 July 2021, accessed 10 November 2023, https://thehill.com/opinion/national-security/3821075-we-need-an-open-source-intelligence-center/

68 Harry Kemsley, "Optimising OSINT for the Intelligence Community", Janes Intelligence Podcast: Episode 80 6 July 2023, accessed 10 November 2023, https://www.janes.com/intelligence-resources/open-source-intelligence-podcasts/podcast-details/optimising-osint-for-the-intelligence-community

69 Andrew Paul, "The CIA is building its own version of ChatGPT", Bloomberg, 27 September 2023, accessed 10 November 2023, https://www.popsci.com/technology/cia-chatgpt-ai/

70 Emily Harding, "Move Over JARVIS, Meet OSCAR Open-Source, Cloud-Based, AI-Enabled Reporting for the Intelligence Community"A Report of the CSIS International Security Program, CSIS, January 2022, accessed 10 November 2023, p. 16 https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/220119_Harding_MoveOverJARVIS_MeetOSCAR_0.pdf?VersionId=NqfrbU05ULzzcySzNHB0pTzsNYw3HdfK

71 Ardi Janjeva, Alexander Harris and Joe Byrne "The Future of Open Source Intelligence for UK National Security", RUSI Occasional Paper, June 2022, accessed 10 November 2023, p 6. https://static.rusi.org/330_OP_FutureOfOpenSourceIntelligence_FinalWeb0.pdf#page=6

Option 2: a separate OSINT organisation within the NIC

This paper argues for a separate OSINT organisation as part of the NIC. There are three main arguments for doing so.

The first flows from the emergence of OSINT as a distinct set of disciplines. A dedicated OSINT organisation would — much like existing Signals Intelligence (SIGINT) and Human Intelligence (HUMINT) organisations — concentrate capability and develop tradecraft. In the words of a former heads of the US National Intelligence Council and Defence Intelligence Agency:

"The intelligence community must make OSINT a true intelligence discipline on par with the traditional functional disciplines … Only then will OSINT have the advocacy, commitment, and structure to move from a cottage industry to the core discipline it must become."[72]

The second argument is that concentrating Australia's OSINT capability in a dedicated organisation would make the most of the particular advantages of this discipline. OSINT and classified intelligence have differing advantages and disadvantages. Some consequently argue that secret intelligence organisations are inherently incapable of fully embracing OSINT.[73] It is not necessary to accept that argument to see that an organisation unencumbered by the bureaucracy and culture of secrecy would be cheaper, faster and able to recruit a more diverse workforce. It could therefore better engage with the explosion of open-source data. That is clear from the extraordinary advances of non-government and commercial OSINT organisations.

The third argument is that an OSINT organisation would allow government to better harness the disruptive power of OSINT. The information revolution and the emergence of OSINT is fundamentally challenging the business of secret intelligence. In addition to providing foundational intelligence, OSINT is creating competitive pressure for secret intelligence organisations. Properly managed, both these factors can be used to sharpen the focus of secret organisations on hard targets and valuable secrets.

The strongest argument against establishing a separate OSINT organisation is that doing so would contradict and undermine intelligence integration. That is, the important goal of reducing the bureaucratic barriers separating different "INTs" rather than establishing new ones. The authors of the UK report argue that creating a centralised OSINT agency would amount to "premature abandonment of the ideal scenario where PAI and OSINT are viewed firmly in the context of the other types of intelligence and integrated into analytical approaches across the UK security community".[74]

But it is not clear why the establishment of a centralised OSINT agency would have this effect, any more than existence of distinct SIGINT and HUMINT organisations does. The way OSINT is viewed and used will ultimately depend on its quality rather than its bureaucratic status. There are good reasons to believe that a dedicated OSINT agency would produce better OSINT. That, in turn, would discourage other NIC agencies from using classified resources for unclassified work. But it need not discourage NIC intelligence officers from developing their OSINT skills — anymore than the existence of ONI's OSIB does.

Optimally integrating OSINT and secret intelligence will be a continuing challenge. The real question is whether this is best done within a single classified organisation like ONI, or between distinct organisations under the wider umbrella of the NIC.

72 Bob Ashley and Neil Wiley, "How the Intelligence Community Can Get Better at Open Source Intel", Defense One, 16 July 2021. Justin Doubleday, "Elevating the open source community in the IC" *Inside the IC*, Podcast: Federal News Network: 28 July 2022, accessed 10 November 2023, https://federalnewsnetwork.com/shows/inside-the-ic-podcast/page/2/

73 Amy Zegart, *Spies, Lies and Algorithms* (Princeton University Press: 1 February 2022) p 238.

74 Ardi Janjeva, Alexander Harris and Joe Byrne "The Future of Open Source Intelligence for UK National Security", RUSI Occasional Paper, June 2022, accessed 10 November 2023, p 35. https://static.rusi.org/330_OP_FutureOfOpenSourceIntelligence_FinalWeb0.pdf

Option 3: an OSINT organisation outside the NIC

Australia could improve its OSINT capabilities by establishing an OSINT organisation outside the NIC or even outside of government. It could also foster a public-private partnership or simply rely on existing non-government OSINT organisations.

It could be argued that producing OSINT is not essentially an intelligence or even a government activity. The government's informational needs extend well beyond national security. Private sector and non-government organisations are already delivering increasingly high-quality OSINT products.

Meeting the OSINT challenge outside the NIC would accord with the argument that OSINT and secret intelligence are incompatible activities. Some members of the CSIS panel expressed concern that even a stand-alone OSINT agency might "never be able to thrive inside IC culture that preferences classified data".[75] A strong exponent of this argument is Chris Rasmussen, the founder of NGA's award-winning OSINT "Tearline" project.[76] He argues for a new OSINT organisation within government, but outside the USIC because "the policy, resourcing, and information technology (IT) priorities of classified operations are incompatible with a world flooded with open and commercial data and cannot scale OSINT toward a cohesive national-level mission".[77]

But this argument reflects the needs of an OSINT practitioner more than it does the needs of government. The strongest argument against this option is that it would make the integration of OSINT and secret intelligence even harder. The government needs intelligence that combines both disciplines. The NIC remains the best framework for managing this integration.

75 Brian Katz, "Maintaining the Intelligence Edge Reimagining and Reinventing Intelligence through Innovation, A Report of the CSIS Technology and Intelligence Task Force", January 2021, accessed 10 November 2023, p. 20 https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/210113_Intelligence_Edge.pdf

76 OSINT Foundation, "NGA's Tearline Awarded OSINT Unit of the Year Award", 1 March 2023, accessed 10 November 2023, https://www.osint-foundation.com/NewsBot.asp?MODE=VIEW&ID=29821

77 Chris Rasmussen "Avoiding the Secrecy Trap in Open Source Intelligence" *Cipher Brief*, 21 March 2023, accessed 10 November 2023, https://www.thecipherbrief.com/column_article/avoiding-the-secrecy-trap-in-open-source-intelligence

Sovereign OSINT

This paper argues for the creation of a dedicated OSINT agency within the NIC. There are many ways this could be done. This section describes how this agency might be organised, where it could be located in the bureaucracy, and what it would do. It uses the name AUSINT — the Australian Unclassified Source Intelligence Agency.

Unlike other OSINT organisations, AUSINT would be unambiguously guided by Australia's national interests. Regardless of how reputable other OSINT organisations are, they are ultimately influenced by other factors, including commercial interests.

AUSINT would produce sovereign OSINT. The AUSINT seal of approval on a media report might be the only difference between sovereign OSINT and a commercial product, but it would be a useful one: providing government with confidence about the contents. AUSINT's methodology would — unlike many non-government organisations — be transparent to the government.

Organisation, structure and classification

Like other NIC agencies, AUSINT should be housed in a Ministerial portfolio (see below) and headed by a Director General (DG AUSINT) and its role defined in legislation. This would clarify how its production of OSINT would and would not be constrained by privacy considerations.

DG AUSINT would report to both the relevant Minister and DG NI. One of the DG AUSINT's main responsibilities would be prioritising competing demands from Ministers and from NIC agencies. These demands could also be mediated by ONI. DG AUSINT might also be given authority to produce public reports where deemed necessary, for example to counter disinformation or otherwise uphold the integrity of the public record.

The classification of AUSINT's operations would probably require a flexible and calibrated approach. The less classified AUSINT's facilities, technology and personnel were, the more it would be able to take advantage of the distinct benefits of the OSINT ecosystem. But it may be necessary to impose information security constraints on AUSINT officers who, for example, need access to secret information in order to better target their OSINT. So, DG AUSINT and DG NI would probably need to make more case-by-case decisions.

Foreign Ministers' portfolio

Although the Prime Minister's portfolio is a logical location for AUSINT, it is also a crowded one. Locating AUSINT in the Foreign Affairs and Trade portfolio (alongside ASIS) would strengthen links between AUSINT and DFAT. Internationally, AUSINT could partner with OSINT-focussed elements of the US State Department's Bureau of Intelligence and Research (Open Source Coordination Unit) and the UK FCO's Open Source Unit.

DFAT's unrivalled international network constitutes a vast but under-utilised source of expertise and information. A growing proportion of this knowledge is openly sourced and unclassified. But this information is typically channelled to Canberra through diplomatic reporting cables, a mode that has changed little since the invention of the telegram. Classified reporting should continue filling the gap between OSINT and secret intelligence but harvesting DFAT's unclassified knowledge requires new mechanisms.[78] AUSINT could, for example, publish draft products as wikis which, for a fixed period of time, any DFAT officer could edit.

78 "The [DFAT capability review] said DFAT should make its reporting and analysis from diplomatic posts 'more accessible through a formal messaging system that attracts greater use by other government agencies, improves the ability to share messages with partner governments, is reliable and provides a more intuitive user interface'": Daniel Hurst, "Australia's diplomatic network has 'serious gaps' and needs boost, review warns" *The Guardian,* 8 May 2023, accessed 10 November 2023, https://www.theguardian.com/australia-news/2023/may/08/australias-diplomatic-network-has-serious-gaps-and-needs-boost-review-warns
Dave Sharma, "Taking Australian Diplomacy Digital", 18 April 2019, accessed 10 November 2023, https://www.aspi.org.au/report/taking-australian-diplomacy-digital

Activities and output

AUSINT should not be imagined simply as an unclassified version of a secret intelligence organisation. The range of activities it could pursue would be much wider (and almost certainly exceed its initial resources). So AUSINT should start small, experiment and scale up based on experience. But AUSINT should be discouraged from replicating activities that private sector organisations can do better.

AUSINT could begin by operating as an information clearing house, disseminating reputable media reports. It could also provide a daily report on the events most consequential to Australia's interests, but this need not take the form of a daily media summary. A report which illuminated the gap between media headlines and issues of greatest importance to Australia would be useful. AUSINT could disseminate OSINT products directly to mobile devices, as US Defence and State Departments already do.[79]

AUSINT could also support DFAT's role in raising awareness, countering disinformation and supporting the integrity of the global information environment.[80] Australian "intelligence diplomacy" includes the dissemination of intelligence to brief "foreign governments … on Australian concerns about Chinese involvement in 5G infrastructure development".[81] Such briefings could be mainstreamed into regular diplomacy using more easily-disseminated AUSINT reports.

AUSINT should, however, produce factual reports rather than public diplomacy or propaganda. There is a risk that public reports could be viewed as propaganda, but this risk would not be mitigated by housing AUSINT elsewhere in the government. AUSINT's reputation for objectivity and accuracy would ultimately depend on the quality of its public reports.

Over time, AUSINT should develop the capability to extract insights from large and fast-moving data sets, including through the use of artificial intelligence. This would likely require AUSINT participation in Australia's current efforts to develop sovereign AI.[82] This capability will become necessary to mitigate and offset national dependence on opaque information processing algorithms owned by the private sector and other nations. National security concerns about the Chinese social media app TikTok are just one manifestation of this problem.

AUSINT should be better able than secret intelligence organisations to assist the government with complex transnational issues. Secret intelligence typically provides only limited insight into problems such as climate change, disease and social movements. OSINT can be more useful because of both the data it draws on and the range of methods it can use.

Because most of its staff would require minimal vetting, AUSINT should be able to draw on a more diverse, and more geographically distributed, workforce. It might even take advantage of crowd-sourced analysis. AUSINT would also have more flexibility than secret intelligence organisations to experiment and advance analytic techniques. This could draw on the latest research about cognition, reasoning, insight, futures and forecasting.[83]

79 https://www.tearline.mil George Seffers, "U.S. State Department To Provide Intelligence via Mobile Devices" Cyber Edge, 1 September 2023, accessed 10 November 2023, https://www.afcea.org/signal-media/cyber-edge/us-state-department-provide-intelligence-mobile-devices

80 Shannon Jenkins, "DFAT to set up disinformation taskforce" *The Mandarin*, 17 June 2020, accessed 10 November 2023, https://www.themandarin.com.au/135202-dfat-to-set-up-disinformation-taskforce/

81 Chris Taylor, "Doing good deeds quietly' The rise of intelligence diplomacy as a potent tool of statecraft" *ASPI Strategic Insights*, October 2023, accessed 10 November 2023, p. 6 https://ad-aspi.s3.ap-southeast-2.amazonaws.com/2023-10/SI183%20Doing%20good%20deeds%20quietly.pdf?VersionId=FsOnsqHIwvgyyoCZRojMvUE1_s0a8vyT

82 Tanya Monro "How can Australia build sovereign capability in AI, and why is it that important?", Adelaide: Australian Institute for Machine Learning: 27 September 2022, accessed 10 November 2023, https://www.adelaide.edu.au/aiml/news/list/2022/07/28/how-can-australia-build-sovereign-capability-in-ai-and-why-is-it-that

83 See: Tim van Gelder et. al. *Analytic Rigour in Intelligence*, Hunt Laboratory for Intelligence Research, University of Melbourne: April 2021, accessed 10 November 2023, https://cpb-ap-se2.wpmucdn.com/blogs.unimelb.edu.au/dist/8/401/files/2021/04/Analytic-Rigour-in-Intelligence-Approved-for-Public-Release.pdf
Adrian Wolferg, "In Pursuit of Insight The Everyday Work of Intelligence Analysts Who Solve Real World Novel Problems", National Intelligence University Research Monograph, Spring 2021, accessed 10 November 2023, https://ni-u.edu/wp/wp-content/uploads/2022/07/NIUMonographWolfberg2022_DNI2022_02011.pdf

Beyond intelligence integration

Adapting Australian intelligence to the information era requires holistic reform with the objective of increasing flexibility and improving the production of both OSINT and secret intelligence.

That requires optimising the relationship between them. Establishing a dedicated OSINT agency is necessary, but insufficient. Australia must also strengthen its intelligence coordination and integration mechanisms. This requires clarifying and strengthening the role and responsibilities of ONI.

ONI should do more than just "integrate intelligence capabilities". It should be charged with optimising the production of intelligence, defined as "information that is useful for national security". To achieve this, ONI should:

- Direct the division of labour between AUSINT and other NIC agencies.
- Ensure that the production of OSINT and secret intelligence is complementary where possible.
- Manage competition between AUSINT and other NIC agencies, to ensure that it remains healthy.
- Broker unavoidable trade-offs between the two disciplines, including to facilitate dissemination.
- Compare the relative usefulness of OSINT and secret intelligence.

Synergies and complementarity

OSINT and secret intelligence should be integrated to produce seamlessly joined intelligence products for decision makers. AUSINT would provide context and foundational intelligence on which other NIC agencies could build. Better OSINT would also enable secret intelligence collectors to understand their operating environment, and analysts to isolate problem sets. It would allow scarce classified resources to be focussed on hard targets and valuable secrets. Conversely, secret intelligence should be used to improve OSINT by directing, validating, contradicting or refining OSINT. AUSINT should locate OSINT that corroborates insights initially derived from secret intelligence. This OSINT could be more easily disseminated to decision makers and international partners.

But such integration would not always be straightforward. OSINT and secret intelligence are different ecosystems and the relationship between them is asymmetric. It is relatively easy to use OSINT to inform secret intelligence, but the reverse is harder because secret organisations cannot share information easily. These problems could be reduced by keeping OSINT under a classified umbrella, but doing so would also limit the NIC's ability to capitalise on the particular advantages of the open-source ecosystem.

Former Acting Director of the CIA Michael Morrel describes how, before the Bin Laden raid, the CIA sought detailed information from OSE about Bin Laden's location, the city of Abbottabad. It masked this request by obtaining equally detailed information about other Pakistani cities.[84] The fact that the CIA found it necessary to conceal its true purpose from OSE, another part of CIA, demonstrates that simply housing OSINT capabilities within a secret organisation does not solve this problem; a more calibrated approach is needed.

Competition and comparison

Encouraging complementarity between AUSINT and other NIC agencies should not preclude healthy competition. Rather, institutional competition should be harnessed to produce the most useful information.

AUSINT's production of OSINT should be used to encourage other NIC organisations to focus on the most valuable secrets and to discourage them from over-classifying information. Rapid advances in private sector GEOINT helped pressure the US NGA to streamline its classification process and enable easier dissemination.[85] The same dynamic can be used within government.

Governments must make hard decisions about resource allocation within the NIC. Comparing the usefulness of OSINT and secret intelligence is difficult, but necessary. Mark Lowenthal has lamented that the "electronic media" sometimes "scooped" the intelligence community because it "put a premium on speed … The intelligence community does not have the same luxury and tends to take more time in preparing its initial report.

Being scooped by the media can lead policy makers to believe, mistakenly, that the media offer much the same coverage as the intelligence community — and at greater speed and less cost".[86]

Whether it is right or wrong for decision makers to think this way, it is evident that many do. So it is pointless to simply reject the comparison. Instead, this dynamic should be harnessed. Secret intelligence should be compared to OSINT, and OSINT to media reports. The concept of useful information provides a rough framework for doing so. "Usefulness" encompasses metrics of accuracy, insightfulness, timeliness, relevance and shareability.

Trade-offs

The NIC's production of OSINT and secret intelligence should be integrated and complementary where possible, but trade-offs will be inevitable. In a more competitive environment, the NIC will need to balance more competing demands at different stages of the intelligence cycle.

Mike Morrel's example of Bin Laden's compound in Abbottabad, described above, illustrates the enduring tension between the need to both obtain information and to hide the act of seeking it. OSINT can be used to focus and refine secret intelligence, but it also creates a risk of alerting adversaries to intelligence gaps. Much can be learnt here from the way the US NGA has — in adapting to rapid advances in private sector GEOINT — made more use of OSINT to "tip and cue" its classified collection.[87]

84 Michael Morell, "Kristin Wood on the intelligence value of open source data — "Intelligence Matters", Podcast: CBS News: 8 March 2023, accessed 10 November 2023, https://www.cbsnews.com/news/kristin-wood-on-the-intelligence-value-of-open-source-data-intelligence-matters/

85 Henry Sokolski, "Over-classification: How Bad Is It, What's the Fix?", Non-proliferation Policy Education Centre: Occasional Paper: 28 March 2023, accessed 10 November 2023, https://npolicy.org/over-classification-how-bad-is-it-whats-the-fix-occasional-paper-2303/

86 Marc Lowenthal, *Intelligence: From Secrets to Policy* (United States, CQ Press, 2006 (7th Edition), p 300.

87 US Government, NGA Media Relations "NGA looks to commercial RF emitter data for non-traditional approach", Public Release Number: 21-893 27 September 2021, accessed 10 November 2023, https://www.nga.mil/news/NGA_looks_to_commercial_RF_emitter_data_for_non-tr.html
Center for Strategic and International Studies, "CSIS Korea Chair Announces Research Partnership with National Geospatial-Intelligence CSIS Korea Chair Announces Research Partnership with National Geospatial-Intelligence Agency (NGA)", 22 May 2018, accessed 10 November 2023, https://www.csis.org/news/csis-korea-chair-announces-research-partnership-national-geospatial-intelligence-agency-nga

Another tension is between speed and accuracy. As Lowenthal points out, secret intelligence moves slower than the media partly because it puts more emphasis on accuracy. But the NIC cannot afford to make the perfect the enemy of the good. Some decisions must be made quickly, and the earlier decision makers receive information, the more likely it is to influence their views.[88] An imperfect intelligence report is generally preferable to unreliable breaking news. In some cases, it will be necessary to provide OSINT reports directly to decision makers before they can be checked against secret intelligence (just as presenting decision makers with raw secret intelligence is sometimes necessary).

Competing imperatives to protect and make use of intelligence will require further trade-offs. Much can be learnt from the war in Ukraine. ONI should learn from ODNI's work to develop mechanisms for proactively disseminating intelligence in useable forms, rather than simply reacting to requests from policy makers. This should include the production of OSINT to corroborate insights initially derived from secret intelligence.

At the same time, efforts to shape the information environment should not undermine the credibility of intelligence. An important difference between Washington's selective intelligence disclosures in the lead up to the 2003 invasion of Iraq and its intelligence diplomacy before Russia's 2022 invasion was that in the case of Ukraine, the US was careful to give allies a fuller picture, including information "that didn't make sense to us" according to DNI Avril Haines.[89]

ONI should be empowered to manage these and other trade-offs. Making them will require difficult case-by-case decisions. But, over time, this should generate a body of experience that could provide the basis for protocols and procedures that improve the management of these risks.

88 Alex Mintz and Karl DeRouen Jr, *Understanding Foreign Policy Decision-Making* (United Kingdom: Cambridge University Press, 2010), p 35.

89 Erin Banco, Garrett M. Graff, Lara Seligman, Nahal Toosi and Alexander Ward, "Something Was Badly Wrong': When Washington Realized Russia Was Actually Invading Ukraine" *Politico*, 24 February 2023, accessed 10 November 2023, https://www.politico.com/news/magazine/2023/02/24/russia-ukraine-war-oral-history-00083757

Conclusion

"Outside [the] niche area for traditional espionage, this century's intelligence war will be about open-source data ... the age of a secret service is over".[90]

Calder Walton, *Spies: The epic intelligence war between East and West*

Every independent review of Australia's intelligence infrastructure undertaken over the last 20 years has noted the ongoing information revolution, but none have recommended major changes to adapt to it. The transfer of DFAT's Open Source Unit to ONA, recommended by the Flood review, was not revisited. The reviews did not address the tension between secret institutions and open-source information. Instead, they urged more strategies, training and technology "to filter, translate, verify, summarise, correlate and contextualise greatly increased volumes of data".[91]

More reform is needed. This paper does not presume to know what the future information environment will look like, but it seems clear that the intelligence structures developed during the Cold War are insufficiently flexible to adapt to this new environment.

A dedicated OSINT agency would reset the NIC's approach to open-source data. It would improve the production of OSINT and secret intelligence, and it could be leveraged to create a more flexible and adaptable intelligence bureaucracy.

If Calder Walton is right, then Five Eyes intelligence structures will be turned inside out. Secret intelligence will become a boutique specialisation within the NIC's larger open-source mission. This paper does not argue for this transformation, but it proposes reforms that would make this — and other futures — more possible.

90 Calder Walton, *Spies: The epic intelligence war between East and West* (Hachette, 2023) p 510.

91 Commonwealth of Australia, Department of the Prime Minister and Cabinet, *Report of the 2017 Independent Intelligence Review* (Australia: Australian Government 2017) 39

Australian National University | NATIONAL SECURITY COLLEGE

Contact

national.security.college@anu.edu.au

nsc.anu.edu.au

@NSC_ANU

National Security College

CRICOS Provider #00120C

TEQSA Provider ID: PRV12002

(Australian University)