Stirling Advisory

E-mail: richard.keir@stirlingadvisory.com.au
Website: www.stirlingadvisory.com.au

ABN: 65 657 724 199
ACN: 657 724 199

2024 Independent Intelligence Review
c/o Department of the Prime Minister and Cabinet
PO Box 6500
Canberra, ACT 2600.

Dear Dr Heather Smith and Mr Richard Maude,

SUBMISSION TO THE 2024 INDEPENDENT INTELLIGENCE REVIEW

Introduction

1. Stirling Advisory is very pleased by the establishment of the 2024 Independent Intelligence Review and to provide this submission.

2. By way of introduction, ***Stirling Advisory*** provides strategic advisory services to the intelligence, space, defence, and national security communities, as well as Australian and international industry who are currently engaged, or want to engage, with these communities. I am the Director of Stirling Advisory and acquired over 30 years of experience as a Royal Australian Air Intelligence Officer, rising to be the first Air Force Intelligence Officer to reach the rank of Air Commodore. I retired from full time service in March 2019 and have since undertaken a range of strategic advisory and consulting work on intelligence, space, defence, and national security matters, as an Air Force reservist, a casual, a sole trader and now through my company, Stirling Advisory.

3. This submission will provide input on two terms of reference through the principle that the NIC should engage with the Australian citizenry not just the government, because by extension, strong governance relies on well-informed citizens. This will in turn increase the relevance of OSINT to the NIC as a tool for doing so, while protecting important classified sources and methods. They are:

a. How effectively the NIC serves, and is positioned to serve, national interests and the needs of Government, including in response to the recommendations of recent reviews relevant to defence and security, and the evolving security environment.

b. 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.

4. In 2021 and 2022 I wrote several blogs for the ASPI *Strategist* and my own company's website on two key matters that I think require more focus on, and interest by, the NIC. They were the requirement for an *Annual National Threat Assessment*, and an *Australian National Intelligence Strategy*. The central idea is that both documents should have publicly releasable unclassified versions instead of only classified non-releasable ones to better inform Australians of the threats they face. Additionally, future Independent Intelligence Reviews will also be able to use the strategy to assess the NIC's actual achievements against its stated objectives.

5. These blogs (each was of two parts) are re-produced below with minor editorial changes (including the use of footnotes) and minor updates and corrections, as some things have changed since they were originally published.

Why Australia Needs a National Intelligence Threat Assessment[1]

6. The 16th of September 2021 will be remembered as the day Australia's strategic status changed forever. The AUKUS security partnership and its headline announcement that the United Kingdom and the United States will assist Australia to acquire nuclear-powered submarines, and no doubt other yet-to-be-announced advanced capabilities, give the country the strategic weight that befits its status as the world's 14th largest economy. Serious countries deal with serious threats in serious ways, and that requires a robust, serious threat assessment process.

7. Eighteen months later, the Defence Strategic Review (DSR) conducted by ex-Minister for Defence, Mr Stephen Smith, and ex-Chief of the Defence Force, Air Chief Marshal Sir Angus Houston (Retired), had its findings and recommendations publicly released on 24 April 2023 in a report titled the *National Defence: Defence Strategic Review 2023*.[2] This was the most important review of Defence since the 1986 Dibb Report and proposed the biggest shifts in defence strategy and capability since the end of the Second World War.

8. The DSR's key strategic assessment, which would have likely come from ONI and DIO assessments, is as follows:

> Australia's strategic circumstances and the risks we face are now radically different [to the past]. No longer is our Alliance partner, the United States, the unipolar leader of the Indo-Pacific. Intense China-United States competition is the defining feature of our region and our time. Major power competition in our region has the potential to threaten our interests, including the potential for conflict. The nature of conflict and threats have also changed.
>
> Regional countries continue to modernise their military forces. China's military build-up is now the largest and most ambitious of any country since the end of the Second World War. This has occurred alongside significant economic development, benefiting many countries in the Indo-Pacific, including Australia. This build-up is occurring without transparency or reassurance to the Indo-Pacific region of China's strategic intent. China's

[1] Originally published as: Richard Keir, *Why Australia Needs a National Intelligence Threat Assessment*, 29 October 2021, https://www.aspistrategist.org.au/why-australia-needs-a-national-threat-assessment/

[2] https://www.defence.gov.au/about/reviews-inquiries/defence-strategic-review

> assertion of sovereignty over the South China Sea threatens the global rules-based order in the Indo-Pacific in a way that adversely impacts Australia's national interests. China is also engaged in strategic competition in Australia's near neighbourhood.
>
> As a consequence, for the first time in 80 years, we must go back to fundamentals, to take a first-principles approach as to how we manage and seek to avoid the highest level of strategic risk we now face as a nation: the prospect of major conflict in the region that directly threatens our national interest. [3]

9. One of the most significant aspects of the recent changes in Australia's strategic circumstances is the rate at which we travelled from an easy economic partnership with China to a point where China felt emboldened enough to issue Australia with its list of 14 grievances.[4] The speed and significance of this shift have of course caught many by surprise—especially the Australian public.

10. How can the government bring the public along for the ride in understanding the most significant changes in Australia's national security environment since the late 1930s in a way that is beyond politics?

11. Because of the rapidity of this change, and the existential nature of the threat to Australia as a sovereign nation, I assess that the government needs to conduct an annual national threat assessment. The process would draw on all sources and the outcomes would aid the development of national security strategy and risk assessments, and, just as importantly, would increase public understanding and awareness of the threats we face. The product of this process would be classified and unclassified versions of the threat assessment.

12. The assessment would take the perception of a threat through a coherent, professionalised, and apolitical process so that we understand what it is—and isn't.

13. Threat assessments, or TAs in the intelligence business, are a key part of the intelligence process and are important artefacts that clearly state the sources and means of threat actors and their assessed intentions. Fundamentally, the concept of threat is built around the notions of capability and intent. For a threat to exist, the actor must have the capability or means to harm you or your interests and the will or intent to inflict that harm.

14. The TA process examines and articulates adversary capabilities and intent using robust analytical techniques, and the result is a statement of the level of threat—low, moderate, high, and so on, with each term having a precise meaning.

15. The threat assessment process is a normal, established, repeatable, updatable, and robust intelligence process and a TA is one of the most common intelligence products.

16. In Australia, we don't have a history of such a public process or document (nor do the other Commonwealth members of the Five Eyes, for that matter). We do, however, have a laudable tradition in making apolitical public policy through publicly available reports by the

[3] Australian Government, *National Defence: Defence Strategic Review 2023*, Canberra, pp.23-24.
[4] https://www.smh.com.au/world/asia/if-you-make-china-the-enemy-china-will-be-the-enemy-beijing-s-fresh-threat-to-australia-20201118-p56fqs.html

Productivity Commission, the Australian National Audit Office, and the Treasury. So why wouldn't we do the same for the most significant of national security threats?

17. Threat assessment as a term is being increasingly used in the contexts of counterterrorism, cybersecurity and, more recently, foreign interference. For example, the *2017 Independent Intelligence Review* employed the term 'threat assessment' only in the context of the National Threat Assessment Centre and its focus on counterterrorism.

18. In a significant change since 2017, the head of the Australian Security Intelligence Organisation (ASIO), Mr Mike Burgess, has in recent years made his organisation's annual threat assessments publicly available.[5]

19. The Australian Signals Directorate (ASD) has released its Annual Cyber Threat Report annually since 2015 (except in 2018). The most recent 2022-23 report was produced in collaboration with ten other government organisations.[6]

20. The ASIO threat assessments are a welcome addition to public awareness but, as per ASIO's remit, they focus on counterterrorism, espionage, and foreign interference. ASD's reports likewise focus on cyber threats.

21. These documents are domestically oriented, specialised, and focused. They aren't threat assessments that span the entire NIC—especially the agencies that have assessment roles. Instead, they are more akin to the US Government's annual Homeland Threat Assessment.[7] They do however show that the NIC can and do make public versions of originally secret documents.

22. In December 2018, as recommended by the *2017 Independent Intelligence Review*, the Office of National Intelligence (ONI) was formed out of its predecessor, the Office of National Assessments (ONA). ONI is responsible for enterprise-level management of the national intelligence community and is the single point of accountability to the prime minister and the cabinet's National Security Committee for all intelligence matters, both foreign and domestic.

23. It therefore makes sense that the head of ONI, the Director-General of National Intelligence, lead the national threat assessment process and coordinate input from across the NIC, and that the assessment's focus be an 'all threats' one.

Developing a National Intelligence Threat Assessment for Australia [8]

24. The benchmark for a national threat assessment is set by the US's Office of the Director of National Intelligence (ODNI). Notably, the leadership and enterprise management role of Australia's ONI was modelled on ODNI.

25. The release of the US Intelligence Community's Annual Threat Assessment is always keenly anticipated. Like the ones before it, the 2023 report is an 'all threats' assessment and includes foreign threats such as China, Russia, Iran and North Korea, as well as transnational

[5] https://www.asio.gov.au/director-generals-annual-threat-assessment-2023
[6] https://www.cyber.gov.au/sites/default/files/2023-11/asd-cyber-threat-report-2023.pdf
[7] https://www.dhs.gov/sites/default/files/2023-09/23_0913_ia_23-333-ia_u_homeland-threat-assessment-2024_508C_V6_13Sep23.pdf
[8] Originally published as: Richard Keir, *Developing a National Intelligence Threat Assessment For Australia*, 2 November 2021, https://www.aspistrategist.org.au/developing-a-national-threat-assessment-for-australia/

threats such as climate change, health security, technology, terrorism, malign foreign influence, migration, and transnational organised crime.[9] It shouldn't surprise anyone that China is clearly identified as the US' most significant threat.

26. It is a whole-of–US Intelligence Community threat assessment that is written as an all-source classified document, then declassified for public release. It's also accompanied by the public testimony of the DNI at a hearing of the Senate Select Committee on Intelligence.[10]

27. An Australian equivalent process would be for the Director-General of National Intelligence to lead an annual whole-of–NIC process by developing an all-source classified national threat assessment for delivery to the Prime Minister and the National Security Committee of Cabinet for them to then develop national security strategy and risk assessments.

28. This document would then be 'sanitised' and made unclassified so it could be tabled in parliament by the Prime Minister and be presented by the Director-General of National Intelligence as public testimony on the threats Australia faces to the Parliamentary Joint Committee on Intelligence and Security and the Joint Standing Committee on Foreign Affairs, Defence and Trade.

29. It would also be posted on ONI's website for public access (there are currently no intelligence assessments on the agency's public website). It's important that this process be, and be seen to be, apolitical and be accompanied by a public information campaign.

30. A publicly releasable national threat assessment would ensure the public understands all the threats to Australia's national security, not just the threat from China, and therefore why the government devotes the resources it does to the Departments of Defence and Home Affairs and the NIC.

31. Currently, if you want to know about threats to Australia, other than the domestic threats of terrorism, espionage, and cybercrime, you must go to a US document and translate them to an Australian viewpoint, or rely on think tanks, academia, or the media to do it for you with all the attendant risks.

32. How to make an all-source classified national threat assessment unclassified for public release? Well, not all intelligence collected by the NIC, and the Australian Defence Force's intelligence, surveillance, and reconnaissance (ISR) capability on its behalf, is classified to begin with. Indeed, much of it is already drawn from publicly available information (PAI) and commercially available information (CAI) sources which is then fused with information collected through secret means.

33. OSINT is already a key collection and analysis discipline—just like signals, human and geospatial intelligence—and has much to offer the national threat assessment process. OSINT is increasingly important as shown in the Russo-Ukraine War and the Israeli-Hamas War.

34. Within government, ONI already operates the Open Source Centre (OSC), which 'collects, interprets and disseminates information relating to matters of political, strategic or

[9] https://www.dni.gov/files/ODNI/documents/assessments/ATA-2023-Unclassified-Report.pdf
[10] https://www.dni.gov/index.php/newsroom/congressional-testimonies/congressional-testimonies-2023/3685-dni-haines-opening-statement-on-the-2023-annual-threat-assessment-of-the-u-s-intelligence-community

economic significance to Australia'.[11] Outside government, there are several commercial providers that already work closely with government by providing OSINT products and services.

35. On the more technical side of things, space-based imagery collection is also no longer the sole remit of government. Commercial vendors now operate satellites capable of capturing high-quality unclassified imagery by night and day in all weather. Radio-frequency transmissions—effectively open-source signals intelligence—are also collected by several commercial satellite operators.

36. Think tanks like the Australian Strategic Policy Institute (ASPI) and online investigators like Bellingcat already very effectively use OSINT to support their work, so why not the NIC in the development of the public version of the national threat assessment?

37. Because OSINT is already used in agencies' intelligence processes and products, a good proportion of the classified national threat assessment will already actually be unclassified. The next part of the process will be sanitising what is from secret sources and methods down to the unclassified level.

38. Basically, when sanitising secret intelligence, NIC analysts will be able to use OSINT from a variety of sources and methods as a guide as to what is and is not classified and then make conscious decisions about what to include in the public version and what to keep secret. In addition, not all the detailed 'evidence' needs to be made public; sometimes only the broad assessment will be made public because the evidence can't be.

39. A move towards developing an annual, apolitical, publicly available national threat assessment, rather than ad hoc speeches and 'announceables' made by officials and politicians, would both inform and focus the public. This process would normalise the strategic threat conversation and hopefully reduce the media hype that tends to accompany such announcements. The assessment would be developed by intelligence professionals and delivered to the public through the Parliament and its committee processes.

40. While a national threat assessment should go hand in hand with an 'all hazards' national security strategy, which Australia last produced in 2013, this is a separate but important debate. It needs to be stated, however, that a national threat assessment is not reliant on a national security strategy, though a national security strategy would be reliant on a national threat assessment.

41. An annual all-threats threat assessment process that produces both classified and unclassified assessments for Australians by Australians will enable the Australian public to be properly informed of the significant 1930s- and 1940s-like changes in Australia's strategic environment—and prepare accordingly.

The Australian National Intelligence Community and Strategy [12]

42. A key purpose of threat assessments is to inform strategy, plans and operations about the capability and intent of actual or potential adversaries. However, threat assessments are

[11] https://www.oni.gov.au/about/our-mission

[12] Originally published as: Richard Keir, *The Australian National Intelligence Community and Strategy*, 30 August 2022, https://www.stirlingadvisory.com.au/post/the-australian-national-intelligence-community-and-strategy

only one of many analytical products developed by an intelligence community that is designed, built, developed, and maintained to fulfil its roles and functions as part of the national security architecture. Such a community is large, broad, complicated, and complex and therefore needs strategy to ensure it is appropriately resourced, organised, and focussed to achieve its objectives. An Australian National Intelligence Strategy (NIS) is therefore required.

43. In Lawrence Freedman's magnum opus on strategy – simply titled *Strategy* – his very first sentences are both powerful and illuminating:

> Everyone needs a strategy. Leaders of armies, major corporations, and political parties have long been expected to have strategies, but now no serious organization could imagine being without one. Despite the problems of finding ways through the uncertainty and confusion of human affairs, a strategic approach is still considered to be preferable to one that is merely tactical, let alone random. Having a strategy suggests an ability to look up from the short term and the trivial to view the long term and the essential, to address causes rather than symptoms, to see the woods from the trees. Without strategy, facing up to any problem or striving for any objective would be considered negligent.[13]

44. While there is no single definition of what strategy is, the Australian Defence Force currently defines strategy as:

> A prudent idea or set of ideas for employing the instruments of national power in a synchronised and integrated fashion to achieve theatre, national, and/or multinational objectives.[14]

45. This is not a bad starting point. During my military career, a model for formulating strategy was summarised as 'ends, ways, and means'. The ends are your desired end state which much be clearly defined. The ways are the courses of action on how the end state is to be achieved. The means are the resources you need to achieve your end state (for example, people, money, and equipment). Defining the desired end state is always the first and most important part of the strategy process; for as Franklin Covey says, you need to 'begin with the end in mind.' Then strategies must be led, monitored, and adjusted where necessary as things change or opportunities arise.

46. In December 2018, as recommended by the *2017 Independent Intelligence Review*, ONI was formed, and the six member Australian Intelligence Community (AIC) was increased to the 10-member National Intelligence Community (NIC). ONI's website states that its '…role is to ensure the National Intelligence Community forms an agile, integrated and data-driven intelligence enterprise that can meet the challenges presented by Australia's evolving strategic and security environment. Given the community is constituted of independent agencies that answer to their respective ministers, our leadership is focused on championing collaboration and collective action.'[15]

47. The enterprise leadership of its 10 members requires a strong strategic approach, but over five years later, it is only quite recently that a classified NIS has been developed (so I

[13] Lawrence Freedman, *Strategy*, Oxford University Press, New York, Unites States, 2013, page ix.
[14] Australian Defence Force Doctrine Document.
[15] https://www.oni.gov.au/about/our-mission

am informally advised). However, there is still no publicly available NIS to inform the public on how the NIC will be shaped, how it will be galvanised into action, and how its progress towards its end state will be guided.

48. In Australia, there appear to be three phenomena when it comes to intelligence strategy.

49. First, there is a very high reliance on the five yearly independent intelligence reviews conducted in 2004, 2011 and 2017 to deliver the catalyst for change to the NIC, and even provide the 'strategy' to the NIC, which is to be executed over the ensuing five-year period. Each review has included a series of recommendations that are then almost always implemented as a 'to do' list. There has never been a recommendation for a NIC-wide strategy, let alone one written for public release. While Australia appears to have the 'ways' in terms of various tasks and initiatives, and the 'means' in terms of budget allocations, the 'ends' have not always been so clear.

50. The second phenomenon to understand when it comes to intelligence strategy is that strategy is often seen as a 'corporate plan', with vision and mission statements, and key performance indicators (KPIs). All NIC agencies have a public website which in turn contain a plethora of information regarding an agency's history, leadership, structure, values, annual reports, executive remuneration, accountability, careers, and personnel information. Some publish a 'corporate plan' because it is required under the Public Governance, Performance and Accountability Act 2013 – such as ASIO and ASD.[16,17] But only one has a published strategy at the unclassified level, AGO.[18] But why does AGO have a published strategy, when the other nine NIC agencies do not? Where is the NIS for AGO's strategy to be nested?

51. The third phenomenon is that despite the creation of ONI and the formation of the NIC, key intelligence matters are still often 'announced' in somewhat 'stove-piped' ways which appear to contradict the purpose of the enterprise structure of the community – which was, after all, the major outcome of the 2017 review. For example, the 2022 REDSPICE announcement was a significant one for ASD's capabilities but how does it fit in with the rest of the NIC's capabilities and desired end state?[19]

52. The presence of a NIS would greatly assist such major capability enhancements by ensuring they are made in the context of a clear NIC end state, and that one part of the enterprise does not get ahead of the others, or even worse, fall behind.

53. So, the NIC appears to rely on the five-yearly independent intelligence reviews for much of its strategy; only one of its 10 agencies has published a strategy but there is no NIS for it to be nested within; and there still appear to be signs of stove-piped NIC capability decisions, despite a focus on the enterprise since 2017.

54. So where is the unifying strategy for the NIC? Australia is clearly capable of developing complex multi-organisational strategies such as the 2020 Cyber Security Strategy, which is currently being updated (by the 2023-2030 Australian Cyber Security Strategy), and the 2022 Counter-Terrorism Strategy, so why doesn't it have one for the NIC?

[16] https://www.asio.gov.au/system/files/2023-06/ASIO%20Corporate%20Plan%202022-26.pdf
[17] https://www.asd.gov.au/about/accountability-governance/publications/asd-corporate-plan-2023-24
[18] https://www.defence.gov.au/about/strategic-planning/defence-geoint-2030
[19] https://www.asd.gov.au/about/what-we-do/redspice

A National Intelligence Strategy for Australia [20]

55. First, let's look at what is widely recognised as the benchmark for what a NIS should look like – the US' *National Intelligence Strategy* published by the ODNI. The Australian ONI's leadership and enterprise management role was modelled on the ODNI, and the US NIS is widely understood by the NIC as a very important document. This begs the question: why doesn't Australia have its own publicly available NIS?

56. The US develops and publishes its NIS every four years. The most recent one was published in 2023.[21] They were also published in 2019, 2014, 2009 and for the first time in 2005. Therefore, in the space of 18 years, the US Intelligence Community has produced five NIS' to Australia's none. Notably, the 2011 and 2017 intelligence reviews would have all had access to two and three US NIS' respectively, with no apparent consideration given to whether a similar approach should be adopted by Australia. Clearly the current 2024 intelligence review will have access to the 2023 NIS.

57. What is in the US' NIS and why is it important? In summary, the NIS states the US IC's vision and mission. The NIS format remained mostly unchanged for several editions, but the 2023 NIS changed its format and focus considerably. The 2023 NIS articulates seven principles of professional ethics for the Intelligence Community and then details the following six goals:

- GOAL 1: Position the IC for Intensifying Strategic Competition.
- GOAL 2: Recruit, Develop, and Retain a Talented and Diverse Workforce that Operates as a United Community.
- GOAL 3: Deliver Interoperable and Innovative Solutions at Scale.
- GOAL 4: Diversify, Expand, and Strengthen Partnerships.
- GOAL 5: Expand IC Capabilities and Expertise on Transnational Challenges.
- GOAL 6: Enhance Resilience.[22]

58. The 2019 NIS was quite different as it instead articulated seven mission objectives – three were foundational as they transcended threats and regions (strategic, anticipatory, and current operations intelligence), and four were specific topical mission objectives (cyber threat intelligence, counterterrorism, counterproliferation, and counterintelligence and security). The 2019 NIS then identified seven enterprise objectives: integrated mission management, integrated business management, people, innovation, information sharing and safeguarding, partnerships and privacy, civil liberties, and transparency.

59. Interestingly, the 2019 NIS objectives were almost the same as the 2014 NIS (by the Obama administration). This shows a significant continuity of objectives over an eight-year period and two very different administrations. Notably, in its conclusion, the 2019 NIS stated that it provides:

[20] Originally published as: Richard Keir, *A National Intelligence Strategy for Australia*, 30 August 2022, https://www.stirlingadvisory.com.au/post/a-national-intelligence-strategy-for-australia
[21] https://www.dni.gov/files/ODNI/documents/National_Intelligence_Strategy_2023.pdf
[22] https://www.dni.gov/files/ODNI/documents/National_Intelligence_Strategy_2023.pdf

> …the IC with the DNI's strategic direction for the next four years, aligns IC priorities with other national strategies, and supports the IC's mission to provide timely, insightful, objective, and relevant intelligence and support to inform national security decisions and to protect our Nation and its interests. The IC must fully reflect the NIS in agency strategic plans, annual budget requests, and justifications for the NIP (the National Intelligence Program). The DNI will assess IC element proposals, projects, and programs toward the objectives of the NIS to realize the IC's vision of a Nation made more secure by a fully integrated, agile, resilient, and innovative Intelligence Community that exemplifies America's values.[23]

60. Whereas in its introduction, the 2023 NIS took a slightly softer approach and states that it:

> …lays out the Intelligence Community's role in supporting the priorities outlined in the President's National Security Strategy and serves as the Community's direction for the next four years as we seek to better serve the Nation.[24]

61. These are powerful words to ensure alignment of such a large and diverse IC. There can be no doubt that such similar words, with the organisational and budgetary authority backing them up, would have a similar impact on the NIC's ends, ways and means.

62. The intelligence debate in Australia generally focusses on technology, policy, privacy, and legislation rather than threat focussed capability and capacity. For example, there is little focus on the NIC's capabilities and readiness to play its role in Australia's national security apparatus, or notably a 2024 IIR term of reference, its readiness for crisis or war. This is very different to the often-obsessive focus on ADF equipment acquisitions, strategy, and operations. There is possibly even greater debate on Australia's diplomatic capability than there is on its intelligence capability.

63. Interestingly, issues of technology, policy, privacy, and legislation broadly correspond to the foci of the US NIS' enterprise objectives and most of the content and recommendations of the past independent intelligence reviews. Indeed, the 2017 review specifically addressed issues such as coordination, intelligence priorities and resource management, evaluation, ICT connectivity, data sharing, accountability to government, workforce, cyber security issues, and science and technology. These are all important, but they are fundamentally at the policy and technical levels.

64. The NIC needs to ask itself bigger strategic questions, and the government needs to ask these questions of the NIC. Questions such as: What is the NIC's strategy to support government policy making in a deteriorating strategic environment with China where there is increasing 'grey zone' complexity and risk? If war does eventuate with China over Taiwan or another regional flashpoint, what is the NIC's capability in supporting 'wartime' decision-making by the government? What is the NIC's capability in supporting and enabling ADF and Allied operations at 'campaign' and 'battle' level? What is the NIC's capability path to conducting all-source intelligence fusion to deliver a fully fused intelligence picture to decision-makers at all levels?

[23] https://www.dni.gov/files/ODNI/documents/National_Intelligence_Strategy_2019.pdf
[24] https://www.dni.gov/files/ODNI/documents/National_Intelligence_Strategy_2023.pdf

65. These questions, and many more like them, may be too much too soon for a public document, but they do need to be asked – even if they are only addressed within the walls of the NIC for now. A NIS is critical in providing the framework – ends, ways and means – to address them.

66. In 2022 I recommended that the next independent intelligence review have a focus on intelligence strategy as a key driver of intelligence capability and capacity, with an orientation towards great power competition, grey zone operations, and high intensity combat operations against a modern adversary. It is pleasing that this was included in this review's terms of reference.

67. I further recommend that the NIC be required to develop a NIS every four years, and that the NIC's performance should be assessed against this strategy by follow-on independent intelligence reviews. This would then address the question of how do you know if you are achieving your objectives, if you don't know what your desired end state is to begin with? Perhaps even the cycle for the development of the NIS could be synchronised with the conduct of independent intelligence reviews.

68. As Lawrence Freedman's said in *Strategy*: 'having a strategy suggests an ability to look up from the short term and the trivial to view the long term and the essential…'[25] As our strategic environment continues to worsen, we need clear-eyed intelligence strategy more than ever. It is time for Australia to have a National Intelligence Strategy.

Conclusion and Recommendations

69. I hope the above arguments on the requirement for an *Annual National Threat Assessment* and an *Australian National Intelligence Strategy* are of use to the Review. I'd like to reiterate that the key proposal here is that both documents have publicly releasable unclassified versions instead of only classified non-releasable ones. This will serve to better inform Australians on the threats they face, and to better inform them as to how the NIC is achieving its critical objectives on their behalf.

70. Stirling Advisory recommends:

a. The Director General National Intelligence be responsible for the development of an 'all threats' *Annual National Threat Assessment* in both classified and unclassified publicly releasable forms.

b. The Director General National Intelligence be required to develop a *National Intelligence Strategy* every four years in both classified and unclassified publicly releasable forms.

c. The NIC's performance should be assessed against the *National Intelligence Strategy* by independent intelligence reviews.

d. The cycle for the development of the *National Intelligence Strategy* should be synchronised with the conduct of future independent intelligence reviews so strategy achievement can be included in the terms of reference of future reviews.

71. I am available to discuss any aspects of this submission.

[25] Lawrence Freedman, Strategy, Oxford University Press, New York, Unites States, 2013, page ix.