

TOO SLOW TO NOTICE

FOUR FIXES FOR A FAST CABINET

OCTOBER 2026

JOHN G HOWARD & REUBEN STEFF



**THE
NEW ZEALAND
INITIATIVE**

www.nzinitiative.org.nz

About the Authors

Major General (Ret) John G Howard, MNZM

Major General (Ret) John G Howard, MNZM, is a Senior Fellow of The New Zealand Initiative and the Managing Director of The Source Consultancy Ltd. Throughout his 40-year career, he served in a full range of Command, Instructional, Staff, Senior Liaison and Operational Appointments, with operational service spanning from Bosnia to Afghanistan.

Major General Howard has served as a planning officer and Senior National Officer in HQ US Central Command (HQ US CENTCOM).

He has held senior staff appointments at both the single-service HQ and the Defence National HQ across strategy, doctrine, policy and capability roles.

Notably, he served as the inaugural Chief of Defence Intelligence for the NZDF and represented New Zealand across Five Eyes intelligence boards and NATO Military Intelligence forums.

His international appointments included Deputy Director for Commonwealth Integration at the US Defense Intelligence Agency (DIA), the only non-American executive officer serving across all 18 US intelligence agencies.

He holds a Master of Management and International Defence Studies and a Master of Strategic Studies.

Reuben Steff

Dr Reuben Steff is Assistant Professor of Geopolitics and International Relations at Mendel University, Brno, Czech Republic. His research includes great power competition, emerging technologies, deterrence theory and New Zealand geopolitics. His latest report is *Small Force, Big Data: Defense AI in New Zealand* (Hamburg: Defense AI Observatory, 2026) and he has published five books including *New Zealand's Geopolitics and the US-China Competition* (Palgrave Macmillan, 2025) and *Emerging Technologies and International Security: Machines, the State, and War* (Routledge, 2020).

He is a regular media commentator and has contributed to policy development processes in New Zealand and is an active participant in security-focused dialogues. For many years he has written on New Zealand's geopolitical and strategic security and can be reached at reuben.steff@mendelu.cz.

Published October 2026 by

The New Zealand Initiative
PO Box 10147
Wellington 6143
New Zealand
www.nzinitiative.org.nz

Views expressed are those of the authors and do not necessarily reflect the views of The New Zealand Initiative, its staff, advisors, members, directors or officers.

Research Note
ISSN 2816-0347

About The New Zealand Initiative

The New Zealand Initiative is an independent public policy think tank supported by chief executives of major New Zealand businesses. We believe in evidence-based policy and are committed to developing policies that work for all New Zealanders.

Our mission is to help build a better, stronger New Zealand. We are taking the initiative to promote a prosperous, free and fair society with a competitive, open and dynamic economy. We develop and contribute bold ideas that will have a profound, positive, long-term impact.

Contents

1. Introduction: the intelligence paradox	1
2. The democratisation of open-source intelligence	1
3. Why New Zealand’s Cabinet cycle cannot keep pace	2
4. The capacity to notice: why AI is now a precondition	2
5. Two ages behind: the international frontier and the Solomon Islands lesson	3
6. Delivering on the 2023 National Security Strategy	4
7. Four changes to close the gap	4
7.1 A National Security Adviser and a Director of National Intelligence	4
7.2 A standing rapid-response process	5
7.3 Pre-delegated ministerial authority	5
7.4 Open-source and AI tradecraft standards	6
8. Conclusion	6
Endnotes	8

1. Introduction: the intelligence paradox

We want to begin with a paradox, because it is the one that ought to trouble ministers more than any single threat named in this year's NZSIS Security Threat Environment assessment.¹ There has never been more actionable intelligence available to the New Zealand Government than there is today, yet the government is not, in any serious sense, digesting it fast enough to matter. By contrast, several comparable systems abroad have already embedded regular strategic briefings at the centre of government. Washington prepares an intelligence brief for the President every day, and Ottawa one for the Prime Minister every week.²

The problem is not what New Zealand knows. It is that the country still runs an industrial-age decision system – sequential, scheduled, paper-bound and built to deliberate rather than to react. It has yet to complete the shift to the information age, and beyond that to make a second shift into the age of intelligence. Some counterparts have already made much of that transition and, in certain cases, developed highly mature systems for turning intelligence into timely decisions.

Recommended position

Cabinet should adopt four changes within the year:

1. appoint a dedicated, permanent National Security Adviser (NSA) and a Director of National Intelligence (DNI), each reporting directly to the Prime Minister;
2. stand up a full-time process able to convene ministers within hours of a named warning indicator being crossed;
3. pre-delegate specific, time-limited authority to ministers for a rehearsed menu of fast-moving contingencies; and
4. fund and mandate formal open-source and AI tradecraft standards.

None of this requires collecting more intelligence – it requires organising to act on what is already known.

2. The democratisation of open-source intelligence

This is not a complaint about secrecy or a plea for more classified collection. It is closer to the opposite. Commercial satellite operators such as Planet Labs and Vantor (formerly Maxar) now photograph almost all of the earth's land surface nearly every day and can image any site at resolutions down to 30 centimetres, detail that was the exclusive preserve of national intelligence agencies a generation ago,³ and they did more to warn the world of Russia's full-scale invasion of Ukraine in February 2022 than any single classified estimate:⁴ journalists, analysts and ordinary citizens were tracking troop concentrations along the border for weeks before the tanks moved, using imagery anyone could buy.

In the week of the invasion, researchers at the Middlebury Institute of International Studies spotted a Russian armoured column near Belgorod on commercial radar imagery. At 3.15am local time on 24 February they watched a "traffic jam" appear on Google Maps on the road from Belgorod to the Ukrainian border. "I think we were the first people to see the invasion," Jeffrey Lewis said. "And we saw it in a traffic app."⁵

Layer that against ship-tracking data, undersea cable mapping, flight-tracking data, leaked or official records of government contracts and purchases, corporate registries, and aggregation and filtering software now capable of sorting that ocean of material in minutes rather than months, and you have

what serious analysts are rightly calling a democratisation of intelligence.⁶ Washington's own intelligence community has titled its open-source strategy "The INT of First Resort".⁷ Additionally, open-source intelligence platforms are now readily available online and offer real-time information flows related to an array of crises and conflicts that anyone can follow. Access is therefore no longer the constraint, but government personnel must have discipline and knowledge to watch the right sources, verify what they publish and swiftly move it into the machinery of government while it still carries decision value.

A capable analyst with a laptop and a subscription can now assemble, in an afternoon, a picture of an adversary's activity that would have required dedicated intelligence assets and a classified channel in 2006. The raw material of statecraft is no longer scarce. What New Zealand lacks is the organisational capacity to turn that abundance into a decision before the warning window closes.

3. Why New Zealand's Cabinet cycle cannot keep pace

Consider how New Zealand's Cabinet system is currently structured to operate. Cabinet committee papers must be lodged with the Cabinet Office by 10am on the Thursday before the meeting at which they are to be considered;⁸ miss that deadline and the paper waits for the following week's cycle, unless a minister goes through the separate, exception-driven process of requesting late lodgement.⁹ That is a sensible discipline for the ordinary business of government, and we do not propose to relitigate it here. But it means the standing architecture of executive decision-making in this country still operates on a weekly cycle, at exactly the moment its information environment has moved to an hourly one. For national security the rhythm is slower still. The committee that now carries the portfolio, the Cabinet Foreign Policy and National Security Committee, is scheduled to meet once in each parliamentary sitting block, "or as required".¹⁰ A system built for weekly deliberation is no longer defensible as it cannot keep pace with a warning window that open intelligence now makes visible to anyone who knows where to look, and that open reporting has already told the world is closing.

The Tasman Sea showed in February 2025 how short such windows have become. A Chinese naval task group gave notice of live firing by radio broadcast rather than through governments. Australia's air-traffic controllers first heard of it from a Virgin Australia pilot who had picked up the broadcast, and 49 flights were diverted that day.¹¹

In short, the nation accepts an industrial-age framework to support strategic decision-making in the information age, something that in the private sector would simply not be tolerated.

4. The capacity to notice: why AI is now a precondition

Speed is only half the problem – we also need the capacity to notice. Warning results from converting immense flows of information into key indicators, each attached to a decision already thought through – it is neither assessment nor collection, and New Zealand does a respectable amount of both while doing very little of this. Nor can the watching be done by hand: open material now exceeds what any analytic workforce can read, let alone one of the smallest in the Five Eyes,¹² which is where uptake and employment of artificial intelligence (AI) stops being aspirational and becomes a precondition – not producing the judgement, but the shortlist on which judgement becomes possible.

Both points are well grounded in the scholarship. Students of strategic surprise have argued for more than half a century that the problem is rarely a lack of warning. Richard Betts concluded in 1978 that because "authorities often hear but dismiss correct estimates, intelligence failure is

inseparable from policy failure”.¹³ Before Pearl Harbor and again before the attacks of 11 September 2001, as James Wirtz notes, data pointing to an attack were already available within the “intelligence pipeline”.¹⁴ Scholars now call this the warning–response gap and ask whether warnings are “noticed, accepted, prioritized and responded to by policy-makers”.¹⁵ Research on AI in intelligence work points the same way. Data analytics “cannot replace the central role of humans and their ability to contextualize security threats”,¹⁶ and cheaper machine prediction makes human judgement more valuable, not less.¹⁷

5. Two ages behind: the international frontier and the Solomon Islands lesson

Worse, the information age is no longer the standard being set. The frontier is moving. Chinese analysts describe a transition from “informatisation”¹⁸ – the networking of the PLA’s forces, sensors and data – to “intelligentisation”¹⁹, in which AI is applied not only to command but to decisions themselves, so that future conflict becomes, as one survey of their writing puts it, “a contest between algorithms”²⁰. Beijing’s 2019 defence white paper put it plainly: “War is evolving in form towards informationized warfare, and intelligent warfare is on the horizon.”²¹ Nor is only China thinking like this. The United States calls it “decision advantage”²² and has built its joint command-and-control and Pentagon AI strategies around accelerating it; NATO calls it “decision superiority”²³; and Australia – New Zealand’s only formal defence ally²⁴ – made decision advantage one of six capability effects in its 2024 National Defence Strategy²⁵, with its Department of Defence defining it as “the ability to make better decisions, faster than any potential adversary”²⁶, and backed it with a Defence AI Centre²⁷ and a data strategy²⁸ carrying the phrase in its title.

New Zealand is therefore not one age behind its environment but two, and it cannot close either gap on a weekly Cabinet cycle. New Zealand does not have to imagine what this mismatch costs; the government watched the cost accrue in real time in the Pacific. The draft security agreement between China and Solomon Islands was leaked and began circulating in open reporting in late March 2022.²⁹ The signals had been public for far longer. Honiara switched recognition from Taipei to Beijing in September 2019. After riots tore through its capital in November 2021, Chinese riot-control equipment and police advisers arrived within about two months.³⁰ On 19 April 2022 Beijing announced that the agreement had been signed.³¹ In the intervening weeks the pact, and its implications for the strategic balance of the South Pacific, was argued out largely in public: in the Australian and international press, in Senate question time in Canberra³² and in urgent, visible diplomacy, including Australia’s dispatch of a minister to Honiara in a late attempt to change the outcome.³³ None of this required a classified source. All it required was someone to read what was already being reported, decide what New Zealand’s response should be, and get a Cabinet-level decision moving inside days rather than weeks. The information was not the constraint. The machinery and culture were.

Ministers did speak quickly. The Prime Minister called the draft agreement “gravely concerning” on 28 March. On 20 April she said the agreement was being signed “with us not having the ability as an Island forum, to address this issue”.³⁴ A faster decision in Wellington would not have guaranteed a different outcome. Honiara acted on its own long-standing security concerns and turned aside Canberra’s late appeal.³⁵ But the pattern has since repeated closer to home, under a different government. New Zealand asked the Cook Islands, a self-governing state in free association with it, for the text of a planned partnership with China in May 2024.³⁶ It had still not seen the text when the Cook Islands Prime Minister signed the agreement in Harbin on 14 February 2025,³⁷ and the decision to pause funding came nearly four months later.³⁸

6. Delivering on the 2023 National Security Strategy

None of this argues for collecting more. It argues for New Zealand ensuring that the vast – and ever-growing – volume of open-source information is turned to advantage rather than left as noise, and doing so in fulfilment of a commitment the Government has already made to itself. New Zealand's 2023 National Security Strategy makes "acting early to prevent national security threats" the first of its three priorities, on the reasoning that "the earlier we can act, the more harm we can prevent",³⁹ and lists strategic competition, foreign interference and espionage, and Pacific resilience and security among its twelve core national security issues. Those three test that commitment most directly. The Solomon Islands case sits squarely inside all three, and the NZSIS's 2026 assessment describes a Pacific that "has become a space contested by major powers".⁴⁰ The current government has kept the Strategy, and DPMC describes its own role as "stewarding the National Security Strategy".⁴¹ Closing the gap this article describes is not a departure from the Strategy; it is what delivering on the Strategy mandates.

7. Four changes to close the gap

Four changes would do more, inside a year, than any additional spending on intelligence gathering.

7.1 A National Security Adviser and a Director of National Intelligence

First and foremost, leadership – establish two key roles.

The National Security Adviser (NSA) – as a stand-alone appointment that reports directly to the PM. This individual should have the professional background, education, experience and exposure to the crafting and delivery of decision support to national-level policy and decision-makers.

The Director of National Intelligence (DNI) – as a stand-alone appointment that reports directly to the PM. This individual should have the professional background, education, experience and exposure to the crafting and delivery of strategic intelligence to national-level policy and decision-makers.

They must be empowered with the appropriate authority and mandate to deliver the necessary strategic changes. They should also have sight of operations, intelligence, setting the National Security Intelligence Priorities (NSIPs),⁴² strategic risks, policy options and consequences simultaneously to put decisions in front of the PM within hours rather than routing them through the lengthy committee cycle.

The idea is not new. In 2020 the Royal Commission of Inquiry into the terrorist attack on Christchurch masjidain recommended a new national intelligence and security agency. Its chief executive would be "designated as the intelligence and security adviser to the prime minister and to Cabinet".⁴³ In 2024 the government decided not to create the agency and instead designated the chief executive of DPMC as National Security Adviser.⁴⁴ It is one of the "many hats" the chief executive says he wears, alongside running the department and chairing ODESC, the National Security Board and the National Hazards Board.⁴⁵ What we propose is a dedicated post.⁴⁶

New Zealand's closest partners have each made at least one of these appointments, and the United States and, since July 2026, Japan have made both (Table 1). Most of these posts date from this century. Australia created its Office of National Intelligence in 2018, after an independent review, and its Director-General leads a ten-agency intelligence community and must keep the Prime Minister informed. In July 2026 Japan added a National Intelligence Council, chaired by the Prime Minister, and a National Intelligence Bureau that answers directly to the Prime Minister's Office. In

August 2025 Germany's cabinet decided to create a National Security Council chaired by the Chancellor.⁴⁷

Table 1: National security advice and intelligence at the centre of government⁴⁸

	National security adviser to the head of government	Central intelligence leadership or assessment	Ministerial national security forum
United States	Since 1953	Director of National Intelligence, since 2005; President's Daily Brief	National Security Council, chaired by the President (1947)
United Kingdom	Since 2010	Joint Intelligence Committee assessments, since 1936	National Security Council, chaired by the Prime Minister (2010)
Canada	Since 2003	Privy Council Office assessment staff produce the Prime Minister's Weekly Intelligence Brief	National Security Council, chaired by the Prime Minister (2023)
Australia	2008–2013	Director-General of National Intelligence, since 2018, who must keep the Prime Minister informed	National Security Committee of Cabinet (1996); its decisions are not normally endorsed by the full Cabinet
Japan	Head of the National Security Secretariat, since 2014	National Intelligence Bureau, directly under the Prime Minister's Office, since 2026	National Security Council (2013); National Intelligence Council, chaired by the Prime Minister (2026)
New Zealand	Title added to the DPMC chief executive's other roles in 2024	National Assessments Bureau, inside DPMC's National Security and Resilience Group	Cabinet Foreign Policy and National Security Committee, chaired by the Minister of Foreign Affairs; scheduled once per sitting block

7.2 A standing rapid-response process

Second, process – New Zealand requires a standing capacity, full time, not ad hoc or one-off activations, that is able to convene under urgency the relevant ministers and ministerial groups within hours of a named warning indicator being crossed. The traditional weekly Cabinet cycle would then ratify that decision afterwards, if necessary, rather than needing to gain it beforehand. This process must be regularly and deliberately stress-tested through robust training and exercise, to include senior officials and the actual decision-makers, against real-world scenarios.

Today the opposite is true. DPMC's National Resilience System Handbook, issued in July, records that there is "no longer a standing Cabinet committee associated with the ODESC system for crisis management". How ministers come together "is based on the event at the time".⁴⁹ Officials can move quickly once a crisis is undeniable. After the first shots in Christchurch on 15 March 2019, the chair of ODESC was told within twenty minutes and convened chief executives three hours later. But ODESC is a committee of officials, and ministers do not attend its meetings.⁵⁰

Comparable governments have built the standing capacity New Zealand lacks. Britain's National Situation Centre, operating in the Cabinet Office since September 2021, uses "automated data pipelines" to "provide insights at pace".⁵¹ Japan's National Security Council holds regular four-minister meetings that also "serve as the forum for crisis management".⁵²

7.3 Pre-delegated ministerial authority

Third, Cabinet should pre-delegate specific, time-limited authority to ministers for a pre-approved and rehearsed menu of fast-moving contingencies – a diplomatic démarche, a public statement of position, the release of a contingency fund, a response by law enforcement or the Defence Force, etc – so that an appropriate and swift initial response never has to wait on a full Cabinet meeting that may be days away and far too late to make a difference.

The constitutional machinery for this already exists. The Cabinet Manual allows Cabinet or the Prime Minister to give a committee or specified ministers “power to act” – “power to take a final decision” – “on a clearly defined item”.⁵³ The Foreign Policy and National Security Committee already holds a standing power to act “where the need for urgent action and/or operational or security considerations require it”.⁵⁴ In Australia, decisions of the National Security Committee of Cabinet are not normally endorsed by the full Cabinet at all.⁵⁵ New Zealand does not lack authority. It lacks a process that triggers that authority on warning rather than in a crisis, and a menu of options worked out, costed and rehearsed before they are needed. When Russia invaded Ukraine in February 2022, New Zealand had no autonomous sanctions regime. Parliament passed the Russia Sanctions Act under urgency on 9 March, thirteen days after the invasion,⁵⁶ and a statutory review in 2025 confirmed that the country still had no general regime.⁵⁷

7.4 Open-source and AI tradecraft standards

Fourth, government should fund and mandate formal open-source and AI tradecraft standards, closing gaps the Inspector-General of Intelligence and Security (IGIS) has already identified. Such standards are not a brake on speed; they are what makes speed usable. A minister asked to act within hours on material an algorithm surfaced from public sources will do so only if the provenance is documented and the judgement can be reconstructed afterwards. Decisions will still have to be taken on incomplete information – that is the nature of acting early – and it is precisely why the standards matter. Their purpose is to tell a minister how much uncertainty they are acting under, not to pretend it does not exist.

The Inspector-General’s findings show where to start. In 2024 he recommended that the NZSIS formalise a framework for assessing specialised open-source collection tools and tighten its procedures for automated collection. The same year he assessed both agencies as having “under-developed operational policy and procedure”.⁵⁸ In July this year his review of the agencies’ use of AI found that neither had enabled AI decision-making. He saw an opportunity to build in protocols supporting oversight “while adoption of this technology is in its early stages”.⁵⁹ Nor do the standards have to be invented from scratch. The United Nations human rights office and the University of California, Berkeley, have published the Berkeley Protocol on Digital Open Source Investigations. It sets out professional standards for “the identification, collection, preservation, analysis and presentation of digital open source information”.⁶⁰ Britain’s Professional Head of Intelligence Assessment publishes a “probability yardstick” that ties words such as “likely” and “highly unlikely” to defined numerical ranges.⁶¹

The evidence favours that kind of precision. When 1,514 forecasts from Canadian strategic intelligence reports were scored against what happened, the analysts proved well calibrated but underconfident, especially on the forecasts that mattered most for policy.⁶² In experiments with national security professionals, decision-makers given numerical probabilities were “less willing to support risky actions and more receptive to gathering additional information”.⁶³

8. Conclusion

New Zealand will never out-collect larger nations, and it does not need to try; the material that matters most is, increasingly, open to anyone. What this country can still choose to do is close the gap between what is knowable, in near-real time, to any analyst with an internet connection, and what its own Cabinet can actually act on. That gap is presently measured in weeks. It should be measured in days and, at times, in hours – and the tools now exist if government personnel know where to look and are empowered to swiftly provide important information to senior officials.

Indeed, officials will at times need to watch streams of incoming information in real time, supported by specialists whose expertise is using AI to rapidly filter and analyse it. It is not clear if New Zealand is cultivating a cadre of personnel that can do this (a topic we will address in a future article).

Strategic relevance, in this decade, belongs to the government that organises itself to act inside the window of opportunity, not the one that writes the best assessment after the window has closed.⁶⁴ New Zealand's partners and competitors alike are already reorganising around that proposition. Wellington has not and is now two shifts behind: an industrial-age Cabinet that never fully entered the information age, facing an environment that is shifting to the age of intelligence. That is a choice about organisation rather than budget – which is precisely why it can be fixed right now.

Endnotes

- ¹ New Zealand Security Intelligence Service (NZSIS), *New Zealand's 2026 Security Threat Environment: An Assessment by the New Zealand Security Intelligence Service* (Wellington: NZSIS, 13 August 2026), 5. Among its assessments: "Geopolitical upheaval is bringing downstream threats to New Zealand's safety and security." <https://www.nzsis.govt.nz/assets/NZSIS-Documents/New-Zealands-Security-Threat-Environment-2026.pdf>
- ² The President's Daily Brief is "a daily summary of high-level, all-source information and analysis on national security issues produced for the president and key cabinet members and advisers": Office of the Director of National Intelligence, "What is the PDB?," <https://www.intelligence.gov/publics-daily-brief/presidents-daily-brief>. In Canada, the Privy Council Office's Intelligence Assessment Secretariat produces the "Prime Minister's Weekly Intelligence Brief": Privy Council Office, "Briefing book for the Clerk of the Privy Council 2023," 17 October 2023, <https://www.canada.ca/en/privy-council/corporate/transparency/briefing-documents/clerk-privy-council-2023.html>
- ³ Planet describes its constellation as "the world's largest fleet offering near-daily 3 m data": Planet Labs, "Planet Constellations," <https://www.planet.com/our-constellations/>. Its documentation records that "In 2017, the Dove fleet achieved near-daily coverage of multispectral imagery over all landmasses": Planet, "PlanetScope," <https://docs.planet.com/data/imagery/planetscope/>. Vantor, the name under which Maxar Intelligence has traded since 1 October 2025, offers 30-centimetre imagery and up to 15 collection opportunities a day over the same location: Vantor, <https://www.vantor.com>, accessed 2 October 2026; Ross Wilkers, "Maxar's name is no more after rebrand," *Washington Technology*, 1 October 2025, <https://www.washingtontechnology.com/companies/2025/10/maxars-name-no-more-after-rebrand/408532/>. Until 2014, US rules allowed DigitalGlobe, later part of Maxar, to sell imagery sharper than 50 centimetres only to the US government: Warren Ferster, "U.S. Government Eases Restrictions on DigitalGlobe," *SpaceNews*, 11 June 2014, <https://spacenews.com/40874us-government-eases-restrictions-on-digitalglobe/>
- ⁴ Commercial imagery "offered timely warning of Russia's initial attack": Peter Dohr, "Responding to OSINT: U.S. Strategy and the Democratization of Intelligence," Center for Strategic and International Studies, 23 April 2026, <https://www.csis.org/blogs/strategic-technologies-blog/responding-osint-us-strategy-and-democratization-intelligence>. It also reinforced an unusual campaign of disclosure. In the weeks before the invasion, Washington and London published their own intelligence on Russian preparations, and President Biden explained on 18 February 2022 that the United States was "calling out Russia's plans loudly and repeatedly": The White House, "Remarks by President Biden Providing an Update on Russia and Ukraine," 18 February 2022, <https://bidenwhitehouse.archives.gov/briefing-room/speeches-remarks/2022/02/18/remarks-by-president-biden-providing-an-update-on-russia-and-ukraine/>. See also Huw Dylan and Thomas Maguire, "Secret Intelligence and Public Diplomacy in the Ukraine War," *Survival* 64, no. 4 (2022): 33–74, <https://doi.org/10.1080/00396338.2022.2103257>, who note that once the invasion began, NATO intelligence communities could monitor Russian forces "with relative ease, given the difficulty of hiding massed-armour movements from various aviation, space and social-media platforms".
- ⁵ Aaron Gordon and Matthew Gault, "Google Maps Live Traffic Showed the Russian Invasion of Ukraine," *Vice*, 24 February 2022, <https://www.vice.com/en/article/google-maps-live-traffic-showed-the-russian-invasion-of-ukraine/>; Middlebury Institute of International Studies, "On Google Maps, Tracking the Invasion of Ukraine," 4 March 2022, <https://www.middlebury.edu/institute/news/google-maps-tracking-invasion-ukraine>
- ⁶ Josh Lubersisse, "Democratized Intelligence: How Open-Source Intelligence is Reshaping Asymmetric Advantage," Irregular Warfare Initiative, 28 August 2025, republished by *Small Wars Journal*, 17 October 2025, <https://smallwarsjournal.com/2025/10/17/democratized-intelligence-open-source-osint-revolution/>; Dohr, "Responding to OSINT", which describes "a modern information environment that partially democratizes intelligence". For a sceptical view, see Damien Van Puyvelde and Fernando Tabárez Rienzi, "The Rise of Open-Source Intelligence," *European Journal of International Security* 10, no. 4 (2025): 530–544, <https://doi.org/10.1017/eis.2024.61>, who argue that because high-end open-source work still demands expertise and advanced tools, "The rise of OSINT is not 'democratising intelligence'." That objection strengthens the case made in the conclusion for a trained cadre of specialists.
- ⁷ Office of the Director of National Intelligence and Central Intelligence Agency, *The INT of First Resort: Unlocking the Value of OSINT – The IC OSINT Strategy 2024–2026* (Washington, DC, 8 March 2024), which

-
- notes that “the open source environment continues to expand and evolve at breakneck speed”, https://archive.dni.gov/files/ODNI/documents/IC_OSINT_Strategy.pdf
- ⁸ Cabinet Office, DPMC, “Cabinet paper 10am Thursday submission deadline,” CabGuide, last updated 31 July 2023, <https://www.dPMC.govt.nz/publications/cabinet-paper-10am-thursday-submission-deadline>. Cabinet itself “usually meets on Mondays”: CabGuide, “What are Cabinet and Cabinet committees,” last updated 17 April 2024, <https://www.dPMC.govt.nz/publications/what-are-cabinet-and-cabinet-committees>
- ⁹ A late paper may be lodged only “if there is a need for urgent consideration and approval has been given by the Prime Minister’s office”: CabGuide, “How to get a late Cabinet paper approved,” last updated 17 April 2024, <https://www.dPMC.govt.nz/publications/how-get-late-cabinet-paper-approved>. See also Cabinet Office, *Cabinet Manual 2023*, paras 5.45 and 5.50–5.51.
- ¹⁰ Cabinet Office, “Cabinet Committees: Terms of Reference and Membership,” CO (24) 1, 30 January 2024, updated 17 August 2026, <https://www.dPMC.govt.nz/sites/default/files/2026-08/co-24-1-cabinet-committees-terms-of-reference-and-membership-17aug2026.pdf>. The committee “meets in the second week of each Parliamentary sitting block, or as required”, while the economic, legislation and social outcomes committees meet “weekly in sitting weeks”.
- ¹¹ Andrew Greene and Stephen Dziedzic, “Chinese gave live fire warning with planes ‘literally flying across the Tasman’,” ABC News, 21 February 2025, <https://www.abc.net.au/news/2025-02-21/chinese-warship-pilot-hazard-east-coast/104966826>; Andrew Greene, “Virgin Airlines pilot first alerted authorities to Chinese live fire danger on Friday,” ABC News, 25 February 2025, <https://www.abc.net.au/news/2025-02-25/virgin-airlines-alerted-chinese-live-fire/104977032>. Australia’s Defence Minister, Richard Marles, said: “We weren’t notified by China, we became aware of the issue during the course of the day.”
- ¹² At 30 June 2025 the NZSIS had a headcount of 403, down from 457 a year earlier, and the GCSB 601: NZSIS, *Annual Report 2025*, 32, <https://www.nzsIs.govt.nz/assets/NZSIS-Documents/NZSIS-Annual-Reports/NZSIS-Annual-Report-2025.pdf>; GCSB, *Annual Report 2025*, 27, <https://www.gcsb.govt.nz/assets/GCSB-Annual-Reports/GCSB-Annual-Report-2025.pdf>
- ¹³ Richard K. Betts, “Analysis, War, and Decision: Why Intelligence Failures Are Inevitable,” *World Politics* 31, no. 1 (1978): 61–89, <https://doi.org/10.2307/2009967>. Betts also argued that organisational solutions cannot prevent intelligence failure. The claim made here is narrower: that organisation can shorten the distance between warning and decision.
- ¹⁴ James J. Wirtz, “Responding to Surprise,” *Annual Review of Political Science* 9 (2006): 45–65, <https://doi.org/10.1146/annurev.polisci.9.062404.170600>. The classic study is Roberta Wohlstetter, *Pearl Harbor: Warning and Decision* (Stanford: Stanford University Press, 1962).
- ¹⁵ Christoph O. Meyer, Florian Otto, John Brante and Chiara De Franco, “Recasting the Warning-Response Problem: Persuasion and Preventive Policy,” *International Studies Review* 12, no. 4 (2010): 556–578, <https://doi.org/10.1111/j.1468-2486.2010.00960.x>. For New Zealand evidence, see John Battersby, “Security Sector Practitioner Perceptions of the Terror Threat Environment before the Christchurch Attacks,” *Kōtuitui: New Zealand Journal of Social Sciences Online* 15, no. 2 (2020): 295–309, <https://doi.org/10.1080/1177083X.2019.1701049>, who found that practitioners’ roles were “complicated by an overarching sense of social, bureaucratic and political complacency toward the threat of terrorism”.
- ¹⁶ Damien Van Puyvelde, Stephen Coulthart and M. Shahriar Hossain, “Beyond the Buzzword: Big Data and National Security Decision-Making,” *International Affairs* 93, no. 6 (2017): 1397–1416, <https://doi.org/10.1093/ia/iix184>. See also Christopher Eldridge, Chris Hobbs and Matthew Moran, “Fusing Algorithms and Analysts: Open-Source Intelligence in the Age of ‘Big Data’,” *Intelligence and National Security* 33, no. 3 (2018): 391–406, <https://doi.org/10.1080/02684527.2017.1406677>
- ¹⁷ Avi Goldfarb and Jon R. Lindsay, “Prediction and Judgment: Why Artificial Intelligence Increases the Importance of Humans in War,” *International Security* 46, no. 3 (2022): 7–50, https://doi.org/10.1162/isec_a_00425
- ¹⁸ Elsa B. Kania, *Battlefield Singularity: Artificial Intelligence, Military Revolution, and China’s Future Military Power* (Washington, DC: Center for a New American Security, November 2017), 4, 12–13 and 16, <https://www.cnas.org/publications/reports/battlefield-singularity-artificial-intelligence-military-revolution-and-chinas-future-military-power>
- ¹⁹ Ibid., 12, describing “intelligentization” as “a new stage in China’s informatization revolution”.
- ²⁰ Kevin Pollpeter and Amanda Kerrigan, *The PLA and Intelligent Warfare: A Preliminary Analysis*, CNA Research Memorandum CRM-2021-U-030806-Final (Arlington, VA: CNA, October 2021), 9: “Some writers envision that warfare will become a contest between algorithms where advantages in algorithms will drive

-
- advantages in war.” <https://www.cna.org/reports/2021/10/The-PLA-and-Intelligent-Warfare-A-Preliminary-Analysis.pdf>
- 21 State Council Information Office of the People’s Republic of China, *China’s National Defense in the New Era* (Beijing: Foreign Languages Press, July 2019), section I, http://english.www.gov.cn/archive/whitepaper/201907/24/content_WS5d3941ddc6d08408f502283d.html; full text at https://newyork.china-consulate.gov.cn/eng/xw/201908/t20190821_4716051.htm
 - 22 US Department of Defense, *Data, Analytics, and Artificial Intelligence Adoption Strategy: Accelerating Decision Advantage* (Washington, DC, released 2 November 2023), https://media.defense.gov/2023/Nov/02/2003333300/-1/-1/1/DOD_DATA_ANALYTICS_AI_ADOPTION_STRATEGY.PDF. See also US Department of Defense, *Summary of the Joint All-Domain Command and Control (JADC2) Strategy* (Washington, DC, March 2022), 1, which describes the ability “to regain and maintain information and decision advantage” as one of the department’s “top priorities”, <https://media.defense.gov/2022/Mar/17/2002958406/-1/-1/1/SUMMARY-OF-THE-JOINT-ALL-DOMAIN-COMMAND-AND-CONTROL-STRATEGY.PDF>. In January 2026 the Pentagon, now also styled the Department of War, issued a new *Artificial Intelligence Strategy for the Department of War: Accelerating America’s Military AI Dominance* (memorandum of 9 January 2026).
 - 23 NATO, “NATO’s Digital Transformation Implementation Strategy 2.0,” 26 May 2026, <https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2026/05/26/natos-digital-transformation-implementation-strategy>. See also NATO, “Alliance Digital Strategy,” 13 January 2026, which aims “to empower Allied leaders and warfighters with information and decision superiority”, <https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2026/01/13/alliance-digital-strategy>
 - 24 Ministry of Foreign Affairs and Trade, “Australia,” <https://www.mfat.govt.nz/en/countries-and-regions/australia-and-pacific/australia>, which describes Australia as “New Zealand’s only formal defence ally”.
 - 25 Commonwealth of Australia, *2024 National Defence Strategy* (Canberra: Department of Defence, April 2024), paras 4.7–4.13. The *2026 National Defence Strategy* keeps “Achieve decision advantage” among the same six capability effects (paras 4.16–4.22). <https://www.defence.gov.au/about/strategic-planning/2024-national-defence-strategy-2024-integrated-investment-program>
 - 26 Department of Defence (Australia), “Harnessing tech to drive faster decisions across Defence,” 5 January 2026, <https://www.defence.gov.au/news-events/releases/2026-01-05/harnessing-tech-drive-faster-decisions-across-defence>. The definition is the department’s own; the National Defence Strategy does not use this wording.
 - 27 Eleanor Dickinson, “Defence’s AI Centre hunts value in 1 billion unstructured documents,” *iNews*, 18 June 2025, <https://www.itnews.com.au/news/defences-ai-centre-hunts-value-in-1-billion-unstructured-documents-617919>, reporting that the department “established an AI centre within its data division at the end of last year”.
 - 28 Department of Defence (Australia), “Defence Data Strategy 2.0: Decision Advantage in the Data Age,” undated, accessed 2 October 2026, <https://www.defence.gov.au/about/strategic-planning/defence-data-strategy-20-decision-advantage-data-age>
 - 29 Andrew Greene, Stephen Dziedzic and Evan Wasuka, “Leaked documents suggest plans for Chinese military presence in Solomon Islands,” ABC News, 24 March 2022, <https://www.abc.net.au/news/2022-03-24/draft-leak-chinese-military-base-solomon-islands/100937632>
 - 30 Sarah Zheng and Lawrence Chung, “Taiwan ends relationship with Solomon Islands after it votes to cut ties,” *South China Morning Post*, 16 September 2019, <https://www.scmp.com/news/china/diplomacy/article/3027420/taiwan-tries-stop-solomon-islands-diplomatic-switch-beijing>; Agence France-Presse, “Riots rock Solomons Islands capital for third day despite peacekeepers,” *France 24*, 26 November 2021, <https://www.france24.com/en/asia-pacific/20211126-riots-rock-solomons-islands-capital-again-despite-australian-troop-deployment>; Ministry of Foreign Affairs of the People’s Republic of China, statement (in Chinese) on the arrival of the first Chinese police supplies in Honiara on 29 December 2021, 1 January 2022, https://www.mfa.gov.cn/web/gjhdq_676201/gj_676203/dyz_681240/1206_681766/1206x2_681786/202201/t20220101_10478270.shtml; Shan Jie and Zhao Juecheng, “Exclusive: China-Solomon Islands police training enhances friendship, law-enforcement capacity after Chinatown losses,” *Global Times*, 28 July 2022, <https://www.globaltimes.cn/page/202207/1271699.shtml>, which dates the Chinese police team’s arrival to 26 January 2022.

-
- ³¹ Ministry of Foreign Affairs of the People's Republic of China, "Foreign Ministry Spokesperson Wang Wenbin's Regular Press Conference on April 19, 2022," https://www.mfa.gov.cn/eng/xw/fyrbt/lxjzh/202405/t20240530_11347266.html. The Solomon Islands Government said the agreement "was signed recently": "Solomon Islands-China security cooperation signed," 20 April 2022, <https://solomons.gov.sb/solomon-islands-china-security-cooperation-signed/>. The exact signing date was not announced.
- ³² Commonwealth of Australia, *Parliamentary Debates*, Senate, 29 March 2022, Questions without Notice, "Solomon Islands" (Senator Penny Wong to Senator Marise Payne), <https://www.openaustralia.org.au/senate/?id=2022-03-29.30.2>
- ³³ Zed Seselja, Minister for International Development and the Pacific, "Statement on Solomon Islands," 13 April 2022, <https://ministers.dfat.gov.au/minister/zed-seselja/media-release/statement-solomon-islands-0>. He visited Honiara on 12–13 April. A US delegation led by Kurt Campbell followed on 22 April, three days after Beijing's announcement: The White House, "Readout of Senior Administration Travel to Hawaii, Fiji, Papua New Guinea, and Solomon Islands," 22 April 2022, <https://bidenwhitehouse.archives.gov/briefing-room/statements-releases/2022/04/22/readout-of-senior-administration-travel-to-hawaii-fiji-papua-new-guinea-and-solomon-islands>
- ³⁴ Kirsty Needham and Lucy Craymer, "New Zealand's Ardern says Solomon Islands-China deal 'gravely concerning'," Reuters, 28 March 2022, <https://www.nasdaq.com/articles/new-zealands-ardern-says-solomon-islands-china-deal-gravely-concerning> (the Prime Minister was speaking to Radio New Zealand); James Baker, "China-Solomons deal crosses a 'very clear line' – Ardern," 1News, 20 April 2022, <https://www.1news.co.nz/2022/04/20/china-solomons-deal-crosses-a-very-clear-line-ardern/>. On 31 May 2022 the United States and New Zealand jointly warned that "the establishment of a persistent military presence in the Pacific by a state that does not share our values or security interests would fundamentally alter the strategic balance of the region": The White House, "United States – Aotearoa New Zealand Joint Statement," 31 May 2022, <https://bidenwhitehouse.archives.gov/briefing-room/statements-releases/2022/05/31/united-states-aotearoa-new-zealand-joint-statement/>
- ³⁵ Patrick Köllner, "Explaining Sender–Receiver Gaps in Signalling: Australia's 'Pacific Step-up' and Solomon Islands' Multi-alignment," *British Journal of Politics and International Relations* 27, no. 1 (2025): 20–42, <https://doi.org/10.1177/13691481241254712>
- ³⁶ "NZ pressed Cook Islands for months over China deals, documents reveal," *Cook Islands News*, 2 September 2025, <https://www.cookislandsnews.com/internal/national/regional/local/economy/new-zealand/nz-pressed-cook-islands-for-months-over-china-deals-documents-reveal/>
- ³⁷ Office of the Prime Minister of the Cook Islands, "Cook Islands and China strengthen bilateral partnership to secure sustainable growth," 14 February 2025, <https://www.pmooffice.gov.ck/2025/02/14/media-release-cook-islands-and-china-strengthen-bilateral-partnership-to-secure-sustainable-growth/>; "Chinese premier meets Cook Islands PM in Harbin," english.www.gov.cn, 14 February 2025, https://english.www.gov.cn/news/202502/14/content_WS67af4e1bc6d0868f4e8efa61.html; Caleb Fotheringham, "'No areas of concern', says Cook Islands PM on NZ's China deal fears," RNZ, republished by *Asia Pacific Report*, 17 February 2025, <https://asiapacificreport.nz/2025/02/17/no-areas-of-concern-says-cook-islands-pm-on-nzs-china-deal-fears/>
- ³⁸ Reuters, "New Zealand suspends US\$11 million Cook Islands funding over China deal," *South China Morning Post*, 19 June 2025, <https://www.scmp.com/news/asia/australasia/article/3314987/new-zealand-suspends-us1097-million-cook-islands-funding-over-china-deal>. The pause, initially of NZ\$18.2 million, was extended in November 2025 to a total of NZ\$29.8 million across two financial years: RNZ, "New Zealand 'reluctantly' extends pause in Cook Islands funding," 9 November 2025, <https://www.rnz.co.nz/news/political/578329/new-zealand-reluctantly-extends-pause-in-cook-islands-funding>. It was lifted after the two governments signed a Defence and Security Declaration on 2 April 2026, under which the Cook Islands will "engage with New Zealand on any requests for defence and security before engagement with other partners": Winston Peters, "New Zealand and Cook Islands sign Defence & Security Declaration," 2 April 2026, <https://www.beehive.govt.nz/release/new-zealand-and-cook-islands-sign-defence-security-declaration>
- ³⁹ Department of the Prime Minister and Cabinet (DPMC), *Secure Together Tō Tātou Korowai Manaaki: New Zealand's National Security Strategy 2023–2028* (Wellington: DPMC, 4 August 2023), priority 1 and para 135, <https://www.dPMC.govt.nz/sites/default/files/2023-11/national-security-strategy-aug2023.pdf>
- ⁴⁰ NZSIS, *New Zealand's 2026 Security Threat Environment*, 8.

-
- ⁴¹ DPMC, *Strategic Intentions 2025/26 to 2029/30* (February 2026), 3, <https://www.dPMC.govt.nz/sites/default/files/2026-02/dPMC-strategic-intentions-2025-26-to-2029-30.pdf>; on continued implementation of the Strategy, DPMC, *Annual Report 2025*, 18, <https://www.dPMC.govt.nz/sites/default/files/2025-11/dPMC-annual-report-2025-v2.pdf>
- ⁴² DPMC, “National Security Intelligence Priorities,” <https://www.dPMC.govt.nz/our-programmes/national-security/national-security-intelligence-priorities>
- ⁴³ Royal Commission of Inquiry into the Terrorist Attack on Christchurch Masjidain on 15 March 2019, *Ko tō tātou kāinga tēnei* (Wellington, 26 November 2020), recommendation 2, <https://christchurchattack.royalcommission.nz/the-report/findings-and-recommendations/chapter-2-recommendations-to-improve-new-zealands-counter-terrorism-effort/>
- ⁴⁴ Hon Judith Collins, “Concluding the Coordinated Government Response to the Royal Commission of Inquiry into the Attacks on Christchurch Mosques,” Cabinet paper FPS-24-SUB-0019, para 15 and appendix A (“A separate agency will not be established. The CE of DPMC has been designated as the National Security Advisor.”), agreed by the Cabinet Foreign Policy and National Security Committee on 25 June 2024 and confirmed by Cabinet on 1 July 2024, proactively released by DPMC on 9 August 2024, <https://www.dPMC.govt.nz/sites/default/files/2024-08/pr-fps-24-sub-0019-concluding-coordinated-govt-response-rcoi.pdf>
- ⁴⁵ DPMC, *Annual Report 2025*, 2: “As Secretary and Chief Executive of the Department of the Prime Minister and Cabinet, I wear many hats, including National Security Advisor to the Prime Minister, Chair of the National Security Board, National Hazards Board, and the Officials’ Committee for Domestic and External Security Coordination (ODESC).”
- ⁴⁶ One of us has made the parallel case for defence AI, where responsibility is “scattered across the capstone documents, the NZDF, central agencies, and industry with no one charged with connecting them”: Reuben Steff, *Small Force, Big Data: Defense AI in New Zealand*, DAIO Study 26/35 (Hamburg: Defense AI Observatory, 2026), 8, https://defenseai.eu/daio_study2635_small_force_big_data_reuben_steff
- ⁴⁷ Federal Government of Germany, “Germany gets a National Security Council,” 27 August 2025, <https://www.bundesregierung.de/breg-en/news/cabinet-security-council-2381754>
- ⁴⁸ United States: Office of the Historian, “History of the National Security Council, 1947–1997,” <https://georgewbush-whitehouse.archives.gov/nsc/history.html>; Office of the Director of National Intelligence, “About,” <https://www.odni.gov/about/>. United Kingdom: “New National Security Council established,” GOV.UK, 12 May 2010, <https://www.gov.uk/government/news/new-national-security-council-established>; “Joint Intelligence Organisation,” GOV.UK, <https://www.gov.uk/government/groups/joint-intelligence-organisation>; The National Archives, administrative history of CAB 56 (Joint Intelligence Sub-Committee, from 1936), <https://beta.nationalarchives.gov.uk/catalogue/id/C3863>. Canada: “Changes in the Senior Ranks of the Public Service and other Appointments,” 12 December 2003, <https://www.canada.ca/en/news/archive/2003/12/changes-senior-ranks-public-service-other-appointments.html>; Prime Minister of Canada, “Prime Minister announces changes to Cabinet committees,” 27 September 2023, <https://www.pm.gc.ca/en/news/news-releases/2023/09/27/prime-minister-announces-changes-cabinet-committees>; “Cabinet Committee Mandate and Membership,” <https://www.pm.gc.ca/en/cabinet-committee-mandate-and-membership>. Australia: Kevin Rudd, “The First National Security Statement to the Parliament,” 4 December 2008, <https://pmtranscripts.pmc.gov.au/release/transcript-16289>; Michael L’Estrange and Stephen Merchant, *2017 Independent Intelligence Review* (Canberra: Department of the Prime Minister and Cabinet, 2017), recommendation 1, <https://www.pmc.gov.au/sites/default/files/resource/download/2017-Independent-Intelligence-Review.pdf>; *Office of National Intelligence Act 2018*, ss 7 and 17; Dennis Richardson, review of the transfer of the 2003 Cabinet records, chapter 7 (Department of the Prime Minister and Cabinet, January 2024), <https://www.pmc.gov.au/resources/review-transfer-2003-cabinet-records-pmc-national-archives-australia/7-national-archives-australia-and-national-security-committee-cabinet>. After the 2013 election the adviser title was dropped and the post became Associate Secretary, National Security and International Policy, in the Department of the Prime Minister and Cabinet: Stephen Easton, *The Mandarin*, 9 September 2015, <https://www.themandarin.com.au/51218-new-challenge-centre-national-security-aged-care/>. Japan: Ministry of Foreign Affairs of Japan, “National Security Council,” https://www.mofa.go.jp/fp/nsp/page1we_000080.html; Chief Cabinet Secretary, press conference of 7 January 2014 (establishment of the National Security Secretariat), https://japan.kantei.go.jp/tyoukanpress/201401/07_a.html; Cabinet Secretariat, page on the National

-
- Intelligence Council and National Intelligence Bureau (in Japanese), https://www.cas.go.jp/jp/gaiyou/jimu/nic_nib.html. New Zealand: DPMC, *Annual Report 2025*; DPMC, “National Security and Resilience Group,” <https://www.dPMC.govt.nz/our-business-units/national-security-and-resilience-group>; CO (24) 1, updated 17 August 2026.
- ⁴⁹ DPMC, *National Resilience System Handbook* (Wellington: DPMC, July 2026), 30, <https://www.dPMC.govt.nz/sites/default/files/2026-07/national-resilience-system-handbook-jul26.pdf>. The handbook replaced the 2016 National Security System Handbook.
- ⁵⁰ *Ibid.*, 34 and 48.
- ⁵¹ Cabinet Office (United Kingdom), *The UK Government Resilience Framework*, updated 4 December 2023, <https://www.gov.uk/government/publications/the-uk-government-resilience-framework/the-uk-government-resilience-framework-html>
- ⁵² Tomohito Shinoda, “Japan’s National Security Policy Making under the Second Abe Cabinet: The Role of the National Security Council/Secretariat,” *Asian Journal of Comparative Politics* 10, no. 4 (2025): 413–428, <https://doi.org/10.1177/20578911251355728>
- ⁵³ Cabinet Office, *Cabinet Manual 2023*, para 5.9, <https://www.dPMC.govt.nz/our-business-units/cabinet-office/supporting-work-cabinet/cabinet-manual/5-cabinet-decision-making/cabinet-committees>
- ⁵⁴ Cabinet Office, CO (24) 1 (updated 17 August 2026), terms of reference of the Cabinet Foreign Policy and National Security Committee.
- ⁵⁵ Dennis Richardson, review of the transfer of the 2003 Cabinet records, chapter 7 (Canberra: Department of the Prime Minister and Cabinet, January 2024), <https://www.pmc.gov.au/resources/review-transfer-2003-cabinet-records-pmc-national-archives-australia/7-national-archives-australia-and-national-security-committee-cabinet>
- ⁵⁶ Cabinet paper “Russia Sanctions Bill: Approval for Introduction”, para 12, and Cabinet minute CAB-22-MIN-0058 (7 March 2022), proactively released by the Ministry of Foreign Affairs and Trade, April 2022, <https://www.mfat.govt.nz/assets/OIA/OIA-2021-22/Proactive-Release-Russia-Sanctions-Bill-Approval-for-Introduction-April-2022.pdf>; Sam Sachdeva, *Newsroom*, 9 March 2022, <https://newsroom.co.nz/2022/03/09/parliament-as-one-on-russia-sanctions/>; Russia Sanctions Act 2022 (2022 No 6), assented to on 11 March 2022, <https://www.legislation.govt.nz/act/public/2022/0006/latest/whole.html>
- ⁵⁷ Ministry of Foreign Affairs and Trade, *Report of the Statutory Review of the Russia Sanctions Act 2022* (June 2025), 8, <https://www.mfat.govt.nz/assets/Countries-and-Regions/Europe/Ukraine/Report-of-the-Statutory-Review-of-the-Russia-Sanctions-Act-2022-June-2025.pdf>
- ⁵⁸ Inspector-General of Intelligence and Security (IGIS), *Review of NZSIS and GCSB Open Source Intelligence Collection: Public Report* (July 2024), <https://igis.govt.nz/assets/Uploads/FINAL-NZSIS-and-GCSB-Open-Source-Intel-Review-PUBLIC-Report-July-2024.pdf>; IGIS, *Annual Report 2023–2024* (October 2024), 6, <https://igis.govt.nz/assets/Annual-Reports/FINAL-IGIS-Annual-Report-2023-2024.pdf>
- ⁵⁹ IGIS, *NZSIS and GCSB Use of Artificial Intelligence: Public Summary* (June 2026, released 8 July 2026), <https://igis.govt.nz/assets/Public-report-Part-2-Review-report-of-the-agencies-use-of-AI.pdf>. The Inspector-General also notes that neither agency is a signatory to the Algorithm Charter for Aotearoa New Zealand.
- ⁶⁰ Human Rights Center, University of California, Berkeley, School of Law, and Office of the United Nations High Commissioner for Human Rights, *Berkeley Protocol on Digital Open Source Investigations* (New York and Geneva: United Nations, 2022), <https://www.ohchr.org/en/publications/policy-and-methodological-publications/berkeley-protocol-digital-open-source>
- ⁶¹ Professional Head of Intelligence Assessment, “Explaining uncertainty in UK intelligence assessment,” GOV.UK, 24 March 2025, updated 20 July 2026, <https://www.gov.uk/government/publications/explaining-uncertainty-in-uk-intelligence-assessment/explaining-uncertainty-in-uk-intelligence-assessment>. The yardstick runs from “remote chance” (up to about 5 per cent) to “almost certain” (about 95 per cent and above). On communicating the limits of AI-derived judgements, see Megan Hughes, Richard Carter, Amy Harland and Alexander Babuta, *AI and Strategic Decision-Making: Communicating Trust and Uncertainty in AI-Enriched Intelligence* (London: Centre for Emerging Technology and Security, Alan Turing Institute, April 2024), <https://cetas.turing.ac.uk/publications/ai-and-strategic-decision-making>
- ⁶² David R. Mandel and Alan Barnes, “Accuracy of Forecasts in Strategic Intelligence,” *Proceedings of the National Academy of Sciences* 111, no. 30 (2014): 10984–10989, <https://doi.org/10.1073/pnas.1406138111>. See also Mandeep K. Dhami, David R. Mandel, Barbara A. Mellers and Philip E. Tetlock, “Improving Intelligence Analysis with Decision Science,” *Perspectives on*

Psychological Science 10, no. 6 (2015): 753–757, <https://doi.org/10.1177/1745691615598511>, which concludes from the decision-science literature that intelligence procedures relying on verbal probabilities are “ineffective”.

⁶³ Jeffrey A. Friedman, Jennifer S. Lerner and Richard Zeckhauser, “Behavioral Consequences of Probabilistic Precision: Experimental Evidence from National Security Professionals,” *International Organization* 71, no. 4 (2017): 803–826, <https://doi.org/10.1017/S0020818317000352>

⁶⁴ The phrase echoes the Pentagon’s aim to “deliver information advantage at the speed of relevance”: US Department of Defense, *Summary of the Joint All-Domain Command and Control (JADC2) Strategy* (March 2022), 1.