

From common threats to narrative defence

An intelligence-led mission approach for Australia–Japan cooperation

Summary

- China's reaction to Japan's May 2026 intelligence reform shows even legitimate democratic reforms in competitor countries will be contested in the information domain.
- Australia and Japan are already targets of state-linked disinformation. For almost a decade, Australia has been building institutional architecture for countering foreign interference. Japan's posture is younger but maturing rapidly, anchored by a new National Intelligence Council and a transparency-led strategic communications.
- The two countries' strengths are genuinely complementary: Australia brings a harder-edged legislative and attribution architecture, while Japan brings deep regional knowledge, including on China, and a valuable perspective on tackling coercion rooted in its economic security policy.
- A focused bilateral counter-disinformation partnership elevated to a standing mission of Australia–Japan cooperation, anchored by Australia's Office of National Intelligence and Japan's new intelligence machinery, would facilitate a shared taxonomy, narrative-tracking capability, agreed attribution thresholds and joint election and crisis-resilience protocols.
- But resilience in the information domain cannot rest on governments alone. A standing Australia–Japan 1.5-track forum on information integrity is also essential to protecting the democratic conditions that allow legitimate debate.

Introduction

Beijing's reaction to Tokyo's May 2026 intelligence reform was immediate and instructive. As Japan has sought to centralise its intelligence community under a new National Intelligence Council, China's state media entities have cast the reform as a revival of Japan's wartime apparatus, and its foreign ministry has warned Japan to heed the lessons of history. The message is unmistakable: even legitimate democratic reform will be contested in the information domain. For Australia and Japan, the question is not whether to deepen intelligence cooperation, but where doing so delivers greatest effect. China's increasingly aggressive behaviour in the information space supplies the answer: countering state-linked disinformation.

The logic follows from what the two countries share. Both are targeted democracies. Both operate in a region where historical grievance, domestic political division and alliance anxiety can be exploited through hostile narratives. Both are already being targeted together.

Beyond its bilateral benefits, a focused Australia–Japan counter-disinformation partnership would sit naturally within the Quad and wider Indo-Pacific resilience agenda. It could underwrite shared threat assessments, narrative tracking, coordinated public attribution, election and crisis resilience and capacity-building with regional partners. Done well, it would do more than rebut false narratives; it would protect the trust, cohesion and political space on which effective democratic statecraft depends.

Australia's approach

Over the past decade Australia has built an institutional architecture: public attribution, transparency mechanisms and a legislative framework designed to expose covert foreign influence to sunlight. The Foreign Influence Transparency Scheme, in force since 2018, requires registration for activities undertaken on behalf of foreign principals and directed at political or government influence.¹ It sits within a counter-foreign interference framework coordinated by the Department of Home Affairs, linking intelligence, law-enforcement and policy agencies.

That architecture is country-agnostic by design: the Australian Security Intelligence Organisation and the broader National Intelligence Community² apply their powers by reference to conduct and threat, not nationality. But the framework's development has been driven by the capacity and willingness of authoritarian states—primarily China—to use disinformation and coercive instruments against Australia and other allies, friends and partners. That pressure has not eased with the stabilisation of bilateral relations with China since 2022.

Protecting electoral integrity has been a particular focus. The Electoral Integrity Assurance Taskforce advises the Australian Electoral Commission on foreign interference, cyber threats and disinformation affecting federal elections.³ There is recognition that the threat is moving: ASIO's 2025 threat assessment warned AI would enable disinformation and deepfakes that would erode institutional trust at greater volume and in less detectable forms, and that agencies would need to stay ahead of that shift.⁴

But resilience hasn't rested on governments alone. Digital platforms participate through voluntary codes overseen by the Australian Communications and Media Authority, and public-facing efforts such as the AEC's Stop and Consider campaign have sought to build civic resistance.⁵ The open question is whether voluntary arrangements can carry the load, or whether enforceable standards will be required.

Australia's intelligence agencies underwrite these efforts operationally and publicly. Ahead of the 2025 federal election, ASIO Director-General Mike Burgess drew the line plainly: 'If a foreign regime tries to meddle in the election by pressuring diaspora groups, directing foreign language newspapers, spreading disinformation on social media or using any of the other tactics sometimes seen overseas, we will know. And we will act.'⁶

Japan's approach

For its part, Japan brings deep regional networks and knowledge, including in relation to China. Its intelligence reforms mean it is developing a more centralised capacity to act on that insight. Tokyo's economic security agenda also offers new ways to manage vulnerabilities and coercion.

Japan is among the most heavily targeted democracies in the Indo-Pacific. Its counter-disinformation posture is younger than

Australia's and built on a different foundation. Where Canberra worked outward from foreign interference legislation, Tokyo has rooted counter-disinformation in its national security doctrine. Japan's 2022 National Security Strategy was its first that named information warfare as a standing threat and committed to a dedicated counter-capability.⁷ That was a decisive shift, but the years since have seen Japan's defences struggle to keep pace with an evolving threat.

The gap was exposed in 2023 when Japan's discharge of treated water from Fukushima Daiichi nuclear power plant, which had been approved by the International Atomic Energy Agency, became the focus of a Chinese information operation. The campaign pushed fabricated imagery across social media to incite fear.⁸ Tokyo's transparency-led response worked, but it was reactive, resource-intensive and run on siloed ministerial fronts.⁹ It was evident that a more synchronised, government-wide capacity would be required to detect and counter sophisticated operations at speed.

Meanwhile, the threat has sharpened. The February 2026 House of Representatives election was the first in Japan to reveal clear signs of social-media-enabled manipulation of public opinion, including networks of accounts linked to a Chinese campaign targeted the incoming government's hawkish line on China. Even if there was no discernible effect on the integrity of the election's conduct and outcome, Japan Nexus Intelligence assessed that those channels confirmed the latent risk of future interference. Across platforms, state-linked accounts continue to push anti-Japan narratives—misrepresenting Japan's defence build-up as a return to colonial militarism and casting doubt about Japan's sovereignty over Okinawa—to corrode trust in the Japan Self-Defense Forces and strain the US alliance.¹⁰

Japan's intelligence restructure provides an institutional answer to some of the constraints in Japan's fragmented approach to countering disinformation. For decades, four core bodies shared intelligence with the Cabinet Intelligence and Research Office (CIRO) on a largely voluntary basis.¹¹ Recent reforms aim to wire them together. On 27 May, the Diet enacted a law creating a National Intelligence Council, chaired by the prime minister, as the apex body spanning national security, counter-espionage and grey-zone threats. CIRO will become a National Intelligence Agency (or Bureau), functioning as this Council's secretariat. These changes are designed to give Tokyo the whole-of-government fusion of intelligence that counter-disinformation work requires.

Prime Minister Sanae Takaichi has framed the reform as a means to prevent crises and protect national interests, arguing that sound policy depends on higher-quality, timely intelligence.¹² The protection extends to the private-sector soft targets exposed to recent technology thefts, such as research institutes, firms and critical infrastructure. The same logic is driving proposals for foreign-investment screening and a mandatory foreign-agent registration scheme, which are steps toward the transparency architecture Australia has adopted.

The reform's harder edges remain unresolved. Oversight and disclosure mechanisms were not settled in parliamentary debates, generating public scepticism about expanded surveillance despite government insistence that the new bodies will protect privacy. Nonetheless, the trajectory is promising. Whether it continues will depend on whether the new agency can pair centralised capability with oversight transparent enough to earn lasting public trust. Japan's maturing intelligence posture complements Australia's harder-edged legislative and attribution architecture, strengthening the case for a focused partnership.

A shared intelligence-led mission approach

Bringing these comparative advantages together will require a focused political decision to make counter-disinformation a standing mission of bilateral cooperation.

That commitment should be made at the leader level, then carried through regular bilateral machinery. A leaders' statement could recognise that hostile information activity is being used to weaken public trust, distort debate about regional security and portray Australia–Japan cooperation as destabilising. To stand the test of time, the statement needs to detail the hostile behaviour, ideally with examples the public can understand. Japanese Defence Minister Shinjiro Koizumi's speech at the Shangri La Dialogue in May 2026 is an example of doing this well.



Image of Shinjiro Koizumi at the Shangri-La Dialogue: Japan Ministry of Defense, [online](#).

Australia and Japan should also commit to deepening coordination between their intelligence, foreign-policy, law-enforcement and electoral-integrity agencies to detect, assess and counter foreign disinformation. This would give officials the authority to allocate resources, resolve classification barriers and move the issue from episodic consultation into routine bilateral practice.

The natural institutional anchor is alignment between ONI and Japan's new NIA. Early cooperation efforts should be deliberately practical. These could include shared threat assessments, regular analyst exchanges, secure channels for rapid incident consultation, and agreed protocols for when

a disinformation campaign becomes a matter requiring coordinated public response.

A first practical move would be to nominate senior officials in both systems as counter-disinformation mission leads, responsible for coordinating across agencies that hold pieces of the problem: intelligence, foreign affairs, home affairs, defence, electoral bodies and strategic communications teams. Australia has used mission-manager approaches in other national-security contexts. The same model, applied bilaterally, would avoid the predictable failure in which everyone agrees, but no one is accountable for turning awareness into action. The time for doing so is right: with Andrew Shearer, Australia's former Director-General of National Intelligence, commencing as Ambassador to Japan in early 2026.



Andrew Shearer アンドリュー・シーラー
@AusAmbJPN



Australia welcomes the passage of legislation to establish a new National Intelligence Council and boost Japan's intelligence capabilities. During her recent visit to Australia, PM Takaichi agreed with PM Albanese on the importance of strengthening   intelligence cooperation.

7:59 PM · May 27, 2026 · 54.9K Views

Post by Ambassador Shearer on his X social media feed.

This won't require Japan to join Five Eyes, nor will it require Australia and Japan to attempt full-spectrum intelligence integration. The model, instead, would be deliberately narrower and more achievable: a bilateral counter-disinformation cell, initially virtual, supported by regular classified and unclassified exchanges. Its work program could begin with four tasks.

- First, establish a shared taxonomy of hostile information activity. Both countries use overlapping but subtly different concepts: disinformation, foreign interference, cognitive warfare, hybrid threats. A common working vocabulary would make joint assessments faster and reduce the risk that agencies talk past one another.
- Second, build a shared narrative-tracking capability focused on the Indo-Pacific. This should monitor recurring themes rather than individual falsehoods: claims that Japan's security reforms mark a return to militarism; accusations labelling Australia as a US proxy; narratives weakening support for Taiwan contingency planning; themes targeting Okinawa, the Pacific or diaspora communities; and efforts to portray democratic security partnerships as escalatory while normalising authoritarian coercion.
- Third, agree to thresholds for coordinated attribution. Not every hostile narrative warrants a public response. But when campaigns are state-linked, target democratic processes or aim to undermine crisis stability, silence can be read as weakness. Australia's attribution experience complements Japan's regional expertise. Together, they could make attribution more credible and harder for hostile actors to dismiss as a unilateral talking point.

- Fourth, develop joint election and crisis-resilience protocols. Elections, major defence announcements, Taiwan-related crises and cyber incidents are all moments when disinformation can have strategic consequences. Officials should know in advance who calls whom, what information can be shared and when leaders should speak publicly. The test is not whether the system produces another communique; it is whether it can act in the first hours of a crisis.

Legislative and oversight dialogue should accompany the operational track. By growing connections between Australia's Parliamentary Joint Committee on Intelligence and Security and its counterparts in the Japanese Diet, the two legislative bodies can oversee democratic safeguards that make stronger intelligence powers politically sustainable: proportionality, transparency, review and mechanisms for distinguishing between action against foreign interference and action against free speech.

But a non-government track is also essential. Disinformation moves through platforms, media ecosystems, universities, business networks and diaspora communities—channels governments can monitor but cannot inoculate. A standing Australia–Japan 1.5-track forum on information integrity would bring officials together with think tanks, technology companies, media organisations, election experts and civil-society representatives, all speaking from a personal standpoint and in a non-official capacity. The new Australia–Japan leadership dialogue that was jointly announced by the two prime ministers in May 2026 could provide a starting point, but a distinct and dedicated forum focused on counter-disinformation is also required to operationalise leader intent in line with the leadership dialogue.

This forum should be funded as a capability, not a one-off conference. If sustained, it could produce annual narrative-risk assessments, run crisis simulations and support researcher exchanges, while also creating a trusted channel for discussing platform behaviour, diaspora targeting and AI-enabled manipulation. Counter-disinformation deserves to be handled with similar institutional seriousness as economic-security cooperation.

Conclusion

Australia and Japan needn't agree on every policy question to recognise that foreign manipulation is designed to narrow their choices, corrode public trust and hinder regional security cooperation.

Both countries can focus their capable, pressure-tested partnership on a mission demanding sustained operational attention: countering disinformation, especially where it is aimed at directly undermining the bilateral strategic partnership. That means shared threat assessments, narrative tracking, coordinated attribution and crisis-response protocols. The objective is not to securitise the information space; it is to protect the conditions under which legitimate democratic debate can occur.

Japan and Australia are targeted together because their strategic alignment matters. That is precisely why they should also respond to state-linked disinformation together.

Notes

- 1 Australian Attorney-General's Department, 'Foreign Influence Transparency Scheme', undated: [online](#).
- 2 Australian Government, 'National Intelligence Community agencies', undated: [online](#).
- 3 Australian Electoral Commission, 'Electoral Integrity Assurance Taskforce', updated 15 June 2026, [online](#).
- 4 Mike Burgess, 'ASIO Annual Threat Assessment 2025', 19 February 2025, [online](#).
- 5 Australian Communications and Media Authority, 'Online disinformation and misinformation', updated 24 September 2025, [online](#); Australian Electoral Commission, 'Stop and Consider', undated, [online](#).
- 6 Burgess, 'ASIO Annual Threat Assessment 2025'.
- 7 Japan Cabinet Secretariat, *National Security Strategy of Japan*, December 2022, [online](#).
- 8 Albert Zhang, 'Japan targeted by Chinese propaganda and covert online campaign', *The Strategist*, 8 June 2023, [online](#).
- 9 Japan Ministry of Foreign Affairs, 'Regarding media report of an alleged fake document of Ministry of Foreign Affairs', 14 August 2023, [online](#).
- 10 Takahiko Kei, 'Disinformation is Beijing's weapon. Japan needs more than fact-checking to counter it', *The Strategist*, 1 May 2026, [online](#); Hsi-Ting Pai, 'When China-Japan disputes arise, Beijing plays the Ryukyus card', *The Strategist*, 30 January 2026, [online](#); ASPI staff and Japan Nexus Intelligence, 'Normalising disinformation: China shifts to overt operations against Japan', *The Strategist*, 28 November 2025, [online](#).
- 11 Japan Cabinet Intelligence and Research Office, 'Intelligence Community of Japan and CIRO', undated, [online](#).
- 12 Japan Prime Minister's Office, 'Prime Minister Takaichi spoke to the press regarding the act to establish a national intelligence council', 27 May 2026, [online](#).

AI contributed no ideas to this report.

Explainers: Are short analyses that raise awareness of both existing and emerging security and defence policy challenges facing Australia and the region.

Cover image: iStockphoto/Oleksii LiskoniH.

ISSN: 3083-2888 (Online) 3083-287X (Print).

First published June 2026.

© The Australian Strategic Policy Institute Limited 2026, www.aspi.org.au.

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