

Building a multilateral cognitive warfare defense network: A collaborative framework for the United States, Japan, and Taiwan



Atlantic Council

**SCOWCROFT CENTER
FOR STRATEGY AND SECURITY**



The **Scowcroft Center for Strategy and Security** works to develop sustainable, nonpartisan strategies to address the most important security challenges facing the United States and the world. The Center honors General Brent Scowcroft's legacy of service and embodies his ethos of nonpartisan commitment to the cause of security, support for US leadership in cooperation with allies and partners, and dedicated to the mentorship of the next generation of leaders.

The **Indo-Pacific Security Initiative (IPSI)** informs and shapes the strategies, plans, and policies of the United States and its allies and partners to address the most important rising security challenges in the Indo-Pacific, including China's growing threat to the international order and North Korea's destabilizing nuclear weapons advancements. IPSI produces innovative analysis, conducts tabletop exercises, hosts public and private convenings, and engages with US, allied, and partner governments, militaries, media, other key private and public-sector stakeholders, and publics.

© 2026 The Atlantic Council of the United States. All rights reserved. No part of this publication may be reproduced or transmitted in any form or by any means without permission in writing from the Atlantic Council, except in the case of brief quotations in news articles, critical articles, or reviews.

ISBN: 978-1-61977-609-8

Please direct inquiries to:

Atlantic Council
1400 L Street NW, 11th Floor
Washington, DC 20005

2026

Author:

Yu-Hao Shen

Cover:

Photo by Hannah Tu on
Unsplash

Acknowledgments

This report and the author's visiting fellowship at the Indo-Pacific Security Initiative were made possible by generous support from Taiwan's Ministry of National Defense. The views expressed within do not necessarily represent the position of the Taiwanese Army or government.

Table of contents

Executive summary	2
Introduction	3
China's military cognitive warfare doctrine and force structure.....	5
CCP military cognitive warfare against Japan and Taiwan	6
Japan.....	6
Taiwan	10
Taiwan and Japan face different cognitive warfare gaps but can offset each other	13
Conclusion and recommendations	15
Appendix A – DISARM Framework overview.....	17
Appendix B – CCP cognitive warfare against Japan and Taiwan: Red actions and blue capabilities.....	18

Bottom lines up front

1. Beijing is pressuring Japan, South Korea, Taiwan, and the Philippines not only with ships and aircraft but also in the cognitive domain—which no multilateral mechanism defends.
2. China has made cognition a military domain, running campaigns through the whole party-state and contracted artificial intelligence firms to exploit fears of US abandonment.
3. First island chain democracies and the United States should share what they see, build civil society into their own response, and train together.

Executive summary

The Chinese Communist Party (CCP) has upgraded the cognitive domain from the “Three Warfares” to a contest for “brain control,” using artificial intelligence (AI)-enabled, party-state-wide influence campaigns that evolve faster than democratic countermeasures. Yet most security cooperation between first island chain nations still focuses on physical threats, leaving a growing gap in multinational defense against malign information operations.

Using the Disinformation Analysis and Risk Management (DISARM) framework to compare China’s military cognitive warfare against Taiwan and Japan, this report finds that both democracies face the limits on available legal tools to regulate hostile content, because of free speech norms and broad public concern about government control over information.

Regulation also cannot keep pace with fast-evolving tactics. Their strengths, however, are complementary. Taiwan offers a mature public-private ecosystem, linguistic proximity, and frontline experience, while Japan contributes stronger internal official coordination, alliance management, and international strategic communication.

This report therefore argues that these advantages should be integrated through a US-supported, multilateral, cognitive warfare defense network across the first island chain. Built on a shared framework and a common operational picture (COP), such a network would help democracies move from isolated, reactive responses toward coordinated early warning and proactive defense.

Introduction

Beijing presses on two fronts but allies cooperate on only one

As China's military power has continued to rise in recent years, its intention to expand control over the surrounding region has also become more apparent. In particular, Beijing has applied frequent and concrete pressure on Japan, South Korea, Taiwan, and the Philippines, the states along and inside the first island chain. This pressure includes multiple large-scale exercises encircling Taiwan, such as Joint Sword-2024A/B, Strait Thunder-2025A, and Justice Mission-2025, as well as repeated clashes with the Philippines in the South China Sea that involved water cannon attacks, boarding and inspection, and even ramming incidents. People's Liberation Army (PLA) warships and aircraft have moved regularly between Japan's Miyako Islands and Okinawa, and PLA warships entered South Korea's jurisdictional waters in the Yellow Sea more than three hundred times in both 2023 and 2024, about three times the 2017 level.¹ China has even unilaterally declared no-sail zones to conduct military training and has carried out live-fire exercises in the Yellow Sea.² The CCP's assertive military posture in the Taiwan Strait, the South China Sea, the East China Sea, and the Yellow Sea—combined with Sino-Russian joint air patrols and Beijing's tacit acceptance of North Korea's accelerated nuclear weapons development—has turned the Indo-Pacific region into a pressure cooker where conflict could erupt at any moment.³

The countries along the first island chain have already accumulated considerable experience in traditional military strategy and cooperation and have participated in various US-led multinational exercises—such as the Rim of the Pacific Exercise (RIMPAC), Shoulder-to-Shoulder, and Freedom Shield—to address regional threats. However, the pressure that the CCP imposes on the first island chain is not limited to the physical domain; its activities in the information and cognitive domains are also expanding rapidly. These efforts seek to undermine the legitimacy of regional armed forces, divide publics from their governments, erode solidarity among democratic states, and damage alliance cooperation. Beijing has even cooperated with North Korea and Russia in the field of information operations, mutually reinforcing and amplifying each other's narratives, in the hope of outcompeting the United States in the West Pacific influence competition without firing a shot and thereby strengthening its regional hegemonic control.⁴ The Office of the Director of National Intelligence's 2025 Annual Threat Assessment further notes that China is using artificial intelligence (AI) to conduct cognitive attacks that generate national security risks.⁵ As these hybrid threats intensify, however, most regional military cooperation still focuses on conventional domains and leaves cognitive defense underdeveloped.

1. "China's Activities in East China Sea, Pacific Ocean, and Sea of Japan," Japan Ministry of Defense, June 2026, https://www.mod.go.jp/en/d_act/sec_env/pdf/ch_d-act_a.pdf; Roh Suk-Jo and Lee Jung-Soo, "Chinese Warships Cross into S. Korea's EEZ over 330 Times in 2024," Chosun, April 30, 2025, <https://www.chosun.com/english/national-en/2025/04/30/3WTFPYSJD5C-5FMNYGVLLDK5MJU/>.
2. Central News Agency (CNA), "China Suddenly Announces Live-Fire Drills in the Yellow Sea from the 17th: Aimed at Sanae Ta-kaichi's 'Taiwan Contingency' Remarks?" YouTube, November 15, 2025, <https://www.youtube.com/watch?v=wk7PJ45euzc>.
3. Joe Varner, "China Is Turning the Indo-Pacific into a Pressure Cooker," Real Clear World, January 3, 2026, https://www.realclearworld.com/articles/2026/01/03/china_is_turning_the_indo-pacific_into_a_pressure_cooker_1156558.html.
4. Tamás Matura, "Sino-Russian Convergence in Foreign Information Manipulation and Interference: A Global Threat to the US and Its Allies," Center for European Policy Analysis, June 30, 2025, <https://cepa.org/comprehensive-reports/sino-russian-convergence-in-foreign-information-manipulation-and-interference/>.
5. "Annual Threat Assessment of the U.S. Intelligence Community," Office of the Director of National Intelligence, March 2025, <https://www.dni.gov/files/ODNI/documents/assessments/ATA-2025-Unclassified-Report.pdf>.

Admiral Samuel Paparo, the commander of US Pacific Command (USPACOM), emphasized that information operations, cognitive operations, and cyber operations already constitute one of the most important “meta trends” reshaping modern conflict, and that these domains must be incorporated into “every plan, every investment, every operation” from the beginning, rather than being “bolted” on at the end as a secondary concern.⁶ Although the United States has signed separate memoranda of cooperation with Japan and South Korea on countering foreign information manipulation, these scattered bilateral arrangements are unlikely to effectively address the rapidly intensifying threats across the region.⁷ This challenge is further compounded by the fact that governments and publics in many countries still have only limited understanding of CCP political propaganda and united front work, making it difficult to propose effective responses on a unilateral basis.⁸ Taken together, these developments both highlight the widening gap between the evolving threat landscape and existing response mechanisms and underscore the urgency and necessity of establishing a transnational information operations cooperation framework among the first island chain countries.

Methodology and analytical framework

To promote a transnational cooperation framework for information operations, establishing a common defensive language is essential. This study adopts the DISARM framework to analyze CCP information campaigns and corresponding defensive options. The framework divides information campaigns into four major phases. For the Red Team, DISARM

breaks down adversary behavior into tactics, techniques, and tasks. For the Blue Team, it maps countermeasures, grouped by response types and meta techniques, directly against specific Red Team tactics.⁹ Detailed codes appear in the appendices.

Scope and case selection

To provide practical insights for the military information operations (IO) community, this report focuses on military level cognitive warfare, information campaigns that directly affect defense resolve, trust in command and control, alliance cohesion, and the will to fight, rather than attempting to cover the full spectrum of general influence operations.

China’s military cognitive warfare is not aimed at any single country; exercises such as its Justice Mission-2025 around Taiwan simultaneously signal deterrent messages to Japan and the United States, underscoring that frontline democracies along the first island chain face a shared cognitive battlespace.¹⁰ This study therefore selects Taiwan and Japan as primary cases: Taiwan as the main testing ground where CCP cognitive tactics and United Front infrastructure are most fully developed, providing rich data for DISARM analysis; and Japan as a major regional power whose evolving stance on Taiwan Strait stability makes it an essential stakeholder for any multilateral defense network.¹¹ It then applies the DISARM Red Framework to analyze vulnerabilities in each country’s military societal information environment and deconstruct representative CCP campaigns and uses the Blue Framework to map main defensive countermeasures, creating a shared coding baseline for comparing threat profiles and responses.

6. Jennifer Hlad, “Three ‘Meta-Trends’ Are Reshaping Warfare, INDOPACOM Commander Says,” *Defense One*, January 13, 2026, <https://www.defenseone.com/threats/2026/01/three-meta-trends-are-reshaping-warfare-indopacom-commander-says/410666>.
7. “U.S. Signs Memorandum of Cooperation with Japan on Countering Foreign Information Manipulation,” US Department of State, press release, December 6, 2023, <https://2021-2025.state.gov/u-s-signs-memorandum-of-cooperation-with-japan-on-countering-foreign-information-manipulation/>.
8. Russell Hsiao, “Red Tide: CCP Propaganda and United Front in the 21st Century: Case Studies in Japan, Singapore, South Korea, Hong Kong, and Taiwan,” LinkedIn, January 2025, https://www.linkedin.com/posts/russellhsiao_after-nearly-six-years-of-research-and-fieldwork-activity-7279583529921855488-3ZNv/.
9. “DISARM Design Guide,” DISARM Foundation, 2021, 2, https://github.com/DISARMFoundation/DISARMframeworks/blob/main/DI-SARM_DOCUMENTATION/00_AMITT_Design_Guide_version1.pdf.
10. Ying-Yu Lin, “PLA Exercises Send Messages to Taiwan, Japan, U.S.: Experts,” *Focus Taiwan*, December 29, 2025, <https://focus-taiwan.tw/politics/202512290018>.
11. Hsiao, “Red Tide,” 8.

China's military cognitive warfare doctrine and force structure

Conceptual upgrade under doctrinal guidance: From the Three Warfares to brain control

Since 2003, when the PLA formally wrote the Three Warfares (public opinion, psychological, and legal warfare) into its political work regulations, Chinese doctrine has steadily moved toward “informationized” and “intelligentized” warfare.¹² Recent PLA writings describe cognition as a “seventh operational domain” and argue that “brain control” is the highest battle for control during warfare, indicating that Beijing treats cognitive warfare as a primary domain of contest and runs aggressive campaigns to impact peacetime social information environments and public perception, rather than using it as a secondary wartime tool.¹³

Party-state-military-civilian integration: The mobilization structure of military cognitive operations

Since Xi Jinping took power, the CCP has framed “public opinion struggle” as a core task. Through a party-state “system-of-systems” bureaucracy, it has integrated propaganda, united front work, intelligence, and a military-diplomatic apparatus to pursue its goals with both military and non-military tools.¹⁴ The Central Propaganda Department controls domestic and external media narratives, while the United Front Work Department builds and exploits physical interpersonal networks to expand social influence.

At the military level, the PLA's political work system transmits central narratives down to theater command political departments and converged media centers, which synchronize traditional media, social platforms, and short video content for troops, local societies, and foreign audiences, while dedicated information and cyberspace

forces provide technical support to secure information superiority and enable cognitive domain operations.

In recent years, CCP cognitive operations have increasingly adopted an outsourced, industrialized model. The US Department of Defense's 2025 report on China's military power notes that the PLA, through military-civil fusion mechanisms, mobilizes Chinese tech giants such as Baidu, Alibaba, and Huawei to conduct influence operations.¹⁵ Taiwan's National Security Bureau also reports that the CCP mobilizes “information technology companies” and “public relations firms” in an attempt to manipulate Taiwanese public opinion.¹⁶ The *Yomiuri Shimbun*, citing internal documents from the Chinese company GoLaxy revealed by Vanderbilt University, points out that the firm has long cooperated with the Chinese government to monitor cyberspace, identify and analyze the psychological tendencies of target individuals, and subsequently use AI to generate fictitious personas tailored to their preferences, engaging in realistic dialogues to influence public opinion.¹⁷ The report also disclosed a 2018 conversation, assessed to be between the director of the PLA Strategic Support Force's 56th Research Institute and the head of an information analysis company, noting that the company controlled between 5.8 million and 6 million Facebook accounts in Taiwan and intended to increase this to 10 million, apparently for the purpose of election manipulation.¹⁸ This trend toward the industrialization of information manipulation allows CCP authorities to conduct cognitive warfare indirectly, making source attribution and accountability significantly more difficult and rendering the threat even more challenging to counter.

12. “China's National Defense in the New Era,” State Council Information Office of the People's Republic of China, July 2019, <http://politics.people.com.cn/BIG5/n1/2019/0725/c1001-31254445.html>.
13. Guo Yunfei, “Contending for ‘Brain Control’: How Future Wars Can ‘Subdue the Enemy without Fighting,’” *PLA Daily*, June 1, 2020, http://www.81.cn/xxqj_207719/xxjt/II/9826822.html
14. Hsiao, “Red Tide.”
15. Jon Harper, “New Pentagon Report on China's Military Notes Beijing's Progress on LLMs,” *DefenseScoop*, December 26, 2025, <https://defensescoop.com/2025/12/26/dod-report-china-military-and-security-developments-prc-ai-llm/>.
16. “Analysis of China's Cognitive Warfare Tactics against Taiwan in 2025,” Taiwan National Security Bureau, January 11, 2026, <https://www.nsb.gov.tw/en/assets/documents/%E6%96%B0%E8%81%9E%E7%A8%BF/3510977a-3c93-4b15-b1f8-246653335a0d.pdf>.
17. Brett Goldstein and Brett Benson, “The GoLaxy Documents: Inside One Chinese Company's AI-Driven Influence Machine,” Vanderbilt University Institute of National Security, last visited July 27, 2026, <https://www.vanderbilt.edu/national-security/wicked-problems-lab/golaxy>.
18. “Taiwan: Encroaching Election Interference—China's Covert Operations Using AI to Steer Public Opinion,” *Yomiuri Shimbun*, December 27, 2025, <https://www.yomiuri.co.jp/world/20251227-GYT1T00067>.

CCP military cognitive warfare against Japan and Taiwan

This section examines how CCP military cognitive warfare targets Japan and Taiwan and how both countries respond. It reviews core vulnerabilities in their military-societal information environments, focusing on the planning and preparation stages of CCP campaigns. It then analyzes one major crisis case for each country and assesses the main defensive measures, showing where resilience is stronger and where critical gaps remain.

Japan

Japan's cognitive fault lines: Clear China threat, divided resolve

In Japan's military societal information environment, the public sees the CCP as a serious threat but holds contradictory attitudes regarding defense policy. Polls indicate that while 68 percent of the Japanese public views China as the primary security threat, there are significant divisions regarding "whether to militarily intervene in a Taiwan contingency" and "increasing the defense budget."¹⁹ These divisions make it easier for CCP cognitive warfare planners to frame any concrete Japanese defense measure as a costly or risky choice and to sow doubts about the direction of Tokyo's security policy.

Okinawa stands out as the sharpest fault line within this broader picture. Up to 85 percent of residents worry that their homeland could become a battlefield once again, as it was in World War II.²⁰ This historical trauma, combined with Okinawans' long-standing dissatisfaction regarding the heavy concentration of US bases and the feeling of being treated as a buffer zone by Tokyo, gives the CCP a strong entry point for cognitive warfare.

Based on these factors, Beijing can pursue three main axes of cognitive attack against Japan. It can magnify the perceived cost of Japanese intervention in a war, raise questions about Tokyo government defense policies and the US–Japan alliance, and evoke historical fears of Japanese imperialism. These narratives lay the foundation for later campaigns that seek to shape domestic debates and alliance cohesion.

The CCP has already built both physical and digital assets in Japan to carry these messages. Since 2017, Chinese consulates have organized more than sixty one-day consular activities, most of them in Okinawa, to build local interpersonal networks. These events help promote narratives about the so-called undetermined status of the Ryukyus and anti-US base sentiment.²¹ China's National Defense Mobilization Law, enacted in 2010, requires Chinese citizens and organizations to provide personnel, resources, and services for national defense once the state declares mobilization.²² Beijing might therefore be able to draw on roughly 1 million Chinese nationals in Japan. This number is four to five times larger than that of Japan's Self-Defense Forces. Chinese nationals in Tokyo are seven times as numerous as the city's police force, which further increases the potential impact of this Chinese diaspora.²³

Beijing has inserted pro-China content into major online portals by impersonating local Japanese news websites, allowing CCP narratives to appear in Yahoo! News Japan and other mainstream outlets and giving them the appearance of local reporting.²⁴ In the purely digital domain, Google has blocked more than two hundred web domains linked to CCP information operations targeting Japanese audiences, and researchers have identified nearly two hundred pro-China fake accounts on the X platform, which often cross-post with pro-Russia accounts to amplify their reach.²⁵ Together, these

-
19. "China Tops Japanese Public's Security Worries in Latest Government Poll," *Straits Times*, January 8, 2026, <https://www.straitstimes.com/asia/east-asia/china-tops-japanese-publics-security-worries-in-latest-government-poll>; "Japanese Divided on Military Response to China over Taiwan, Kyodo Poll Shows," Reuters, November 16, 2025, <https://www.reuters.com/world/china/japanese-divided-military-response-china-over-taiwan-kyodo-poll-shows-2025-11-16>.
 20. Kenji Yoshida, "Caught in the Crosshairs, Okinawa Faces the Taiwan Test," *JAPAN Forward*, January 13, 2026, <https://japan-forward.com/caught-in-the-crosshairs-okinawa-faces-the-taiwan-test>.
 21. "National Defense Mobilization Law of the People's Republic of China, adopted February 26, 2010, effective July 1, 2010," National People's Congress, 2010, http://www.npc.gov.cn/cwhhdbdh/c4186/c12576/c12587/201905/t20190523_403603.html.
 22. "Japan Targeted by China's Gray-Zone Influence Operations," Global Influence Operations Report, November 20, 2025, <https://www.global-influence-ops.com/china-gray-zone-influence-operations-target-japan/>.
 23. Kenji Yoshida, "Robert Eldridge: How China Seeks to Win without Firing a Shot," *JAPAN Forward*, January 22, 2026, <https://japan-forward.com/robert-eldridge-how-china-seeks-to-win-without-firing-a-shot>.
 24. "Japan Targeted by China's Gray-Zone Influence Operations."
 25. Dylan J. Plung and Kenton Thibaut, "Japan's Technology Paradox: The Challenge of Chinese Disinformation," Digital Forensic Research Lab, March 25, 2025, <https://dfirlab.org/2025/03/25/japan-tech-chinese-disinformation>.

physical and online channels allow Beijing to export narratives that look like local public opinion and can be quickly mobilized when a crisis or incident provides a trigger.

Takaichi's remarks triggered a multilayered cognitive campaign against Japan

Following Japanese Prime Minister Sanae Takaichi's remarks in November 2025 that a conflict in the Taiwan Strait would constitute a "survival-threatening situation" for Japan, bilateral diplomatic relations deteriorated rapidly. This incident simultaneously triggered a multilayered CCP military cognitive warfare campaign against Japan.²⁶ This campaign consisted of three main lines of attack: diplomatic and legal intimidation, manipulation of the Okinawa issue, and dividing the regional alliance.

First, Beijing sought to set the tone by using aggressive diplomacy to intimidate Japan's decision-makers. This

included severe condemnations by the Chinese Ministry of Foreign Affairs and "wolf warrior" tactics, such as the consul general in Osaka posting extreme remarks calling for Takaichi to be "beheaded."²⁷ Concurrently, the CCP repeatedly invoked the "enemy state clauses" of the United Nations (UN) Charter to wage legal warfare, asserting that the prime minister's statements signaled a return to wartime aggression. The purpose was to recast a legitimate defense debate as a dangerous sign of revived militarism and to raise the political cost of firmer Japanese positions on Taiwan.

Second, Beijing used Okinawa as the main local pressure point. It issued a travel advisory warning citizens against visiting Japan and then mobilized state media to push claims that "Okinawa's tourism has been severely hit."²⁸ Simultaneously, Chinese accounts flooded social media platforms with more than ten thousand posts declaring, "Ryukyu is not a part of Japan" and "don't be used as a battlefield again."²⁹ State media also repeatedly amplified narratives questioning Okinawa's sovereignty to maximize the reach of their attacks, aiming to produce contradictions and distrust between Tokyo and Okinawa by connecting local livelihood concerns and historical disputes with the central defense policy discussions.³⁰

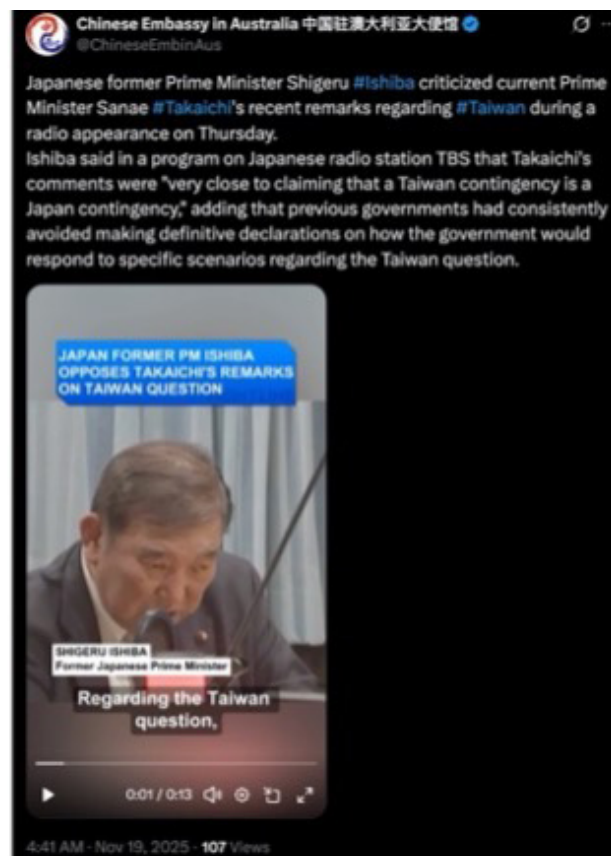


A wolf warrior post on X by China's consul general in Osaka responding to Takaichi's remarks. Credit: @xuejianosaka, X post, archived by archive.today.



A travel warning against visiting Japan published on the official website of the Chinese Embassy in Japan. Credit: Embassy of the People's Republic of China in Japan.

26. Takashi Hosoda, "China's 'Special Cognitive Warfare Operation' Against Japan and Its Trajectory," Sinopsis, January 8, 2026, <https://sinopsis.cz/en/chinas-special-cognitive-warfare-operation-against-japan-and-its-trajectory/>.
27. Xue Jian (@xuejianosaka), X post (post deleted), November 8, 2025 (post deleted), <https://archive.today/20251109043835/https://x.com/xuejianosaka/status/1987168322170052963>.
28. "Advisory on Avoiding Travel to Japan in the Near Term," Embassy of the People's Republic of China in Japan, November 14, 2025, https://jp.china-embassy.gov.cn/zytz_0/202511/t20251114_11753712.htm; "Okinawa Tourism Body Calls Takaichi's Taiwan Remarks 'Regrettable,' Hopes for Quick Stabilization," *Global Times*, November 19, 2025, <https://www.globaltimes.cn/page/202511/1348597.shtml>.
29. Daisuke Furuta, "False Information about Japan-China Relations Surged after Takaichi's Remarks: Manipulated Videos Stoke 'Ryukyu Independence' in a Cognitive Warfare Campaign," Japan Fact-Check Center, December 6, 2025, <https://www.factcheckcenter.jp/explainer/international/cognitive-warfare-after-takaichi-taiwan>.
30. Chen Qingqing, "Deepening Research on Ryukyu History Continues to Carry Significant Contemporary Value for China-Japan relations," *Global Times*, November 18, 2025, <https://www.globaltimes.cn/page/202511/1348510.shtml>.



Four video posts attacking Japan published within two days on the X account of the Chinese Embassy in Australia. Credit: X/@ChineseEmbinAus, screenshots compiled by the author.

Third, on the international stage, the CCP attempted to frame Japan as a troublemaker reviving militarism. For example, the X account of the Chinese Embassy in Australia claimed that joint exercises between the United States, Japan, and Australia were “preparing for war” and warned Australia of the risk of being “dragged into conflict.”³¹ China’s state media apparatus simultaneously linked Japan’s current defense affairs with wartime militarism, asserting that Japan is resuming militaristic expansion.³² This cross-border narrative projection was intended to undermine alliance trust in the Indo-Pacific region.

Japan’s cognitive defense: Strong at the top but weaker at home

Faced with China’s cognitive warfare, the Japanese government no longer adopts a purely passive response posture; it instead treats cognitive warfare as a national security issue and incorporates it into its overall strategic architecture. It not only identified cognitive warfare as a threat in the 2022 revision of the National Security Strategy but also established a cross ministerial response mechanism under which the Ministry of Foreign Affairs (MOFA) and the Ministry of Defense (MOD) conduct monitoring, the Cabinet Intelligence and Research Office (CIRO) performs analysis, and the chief cabinet secretary leads external communication.³³ On the military side, the Defense Intelligence Headquarters (DIH) serves as the core node, integrating the Japan Joint Operations Command (JJOC) and information operations units across the services, with plans to establish an integrated information warfare mechanism within the Self Defense Forces by 2027.³⁴ This top down integration and division of labor strengthen Japan’s ability to detect Chinese information operations and reflect high level political attention and commitment in terms of strategic planning and institutional design.

Japan also actively leverages its alliance network and diplomatic resources to respond to Chinese cognitive warfare. As a Group of Seven (G7) member, Japan published the report

“Existing Practices against Disinformation (EPaD)” in 2023 to compile the practical experiences of member states.³⁵ At the same time, Tokyo has built bilateral cooperation on countering foreign information manipulation and interference (FIMI) with the United States, Australia, Thailand, and others, and has promoted information operation exchanges through multilateral frameworks such as the US–Japan–South Korea trilateral, the Quad, and NATO.³⁶ In the military field, the Japan Maritime Self-Defense Force (JMSDF) signed an information warfare cooperation memorandum with the US Pacific Fleet and the Royal Australian Navy in 2024 and jointly participated in the Blue Spectrum information warfare exercise, which strengthened Japan’s experience in multinational information operations. In concrete crises such as the CCP cognitive warfare campaign that followed Takaichi’s November 2025 remarks on Taiwan, Japan has also been able to use diplomatic channels, sending letters to the UN and lodging formal protests with Beijing to rapidly issue counternarratives and degrade the impact of China’s lawfare and political intimidation.

However, Japan’s domestic defense remains more limited. Its response to united front activities and digital threats is constrained by limited legal tools and public unease toward government regulation in a democratic system, particularly Japanese society’s long-standing postwar sensitivities around security policy. Tokyo still lacks dedicated digital governance legislation targeting disinformation and deepfake content, as well as a foreign agents registration regime to regulate one day consulates, friendship associations, and other united front activities. As a result, authorities face real difficulty in tracking activities and funding flows of proxy networks, restricting coordinated malicious behavior, and forcing the removal of harmful content inside Japan’s information space.

At the societal level, although Japan’s linguistic environment and ingrained skepticism give the public a degree of accidental resilience against disinformation, the country still faces the problem of insufficient civic participation when dealing with mixed true and false narratives and on the ground united

-
31. “Normalising Disinformation: China Shifts to Overt Operations against Japan,” Australian Strategic Policy Institute and Japan Nexus Intelligence, November 28, 2025, <https://www.aspistrategist.org.au/normalising-disinformation-china-shifts-to-overt-operations-against-japan/>.
 32. Zhu Chengshan, “Distorted View of History Fuels Takaichi’s Arrogant Remarks on Taiwan,” *People’s Daily*, November 24, 2025, <https://en.people.cn/n3/2025/1124/c90000-20394288.html>; “Takaichi’s Taiwan Remarks Reopen Wounds of Japan’s Wartime Legacy,” CGTN, November 21, 2025, <https://news.cgtn.com/news/2025-11-21/Takaichi-s-Taiwan-remarks-reopen-wounds-of-Japan-s-wartime-legacy-1ltBjpMh6IW/p.html>.
 33. Kyoko Kuwahara, “Japan’s Struggle against Disinformation,” Macdonald-Laurier Institute, March 27, 2025, <https://macdonaldlaurier.ca/japans-struggle-against-disinformation-kyoko-kuwahara-for-inside-policy/>; Maiko Ichihara, “China’s ‘Malinformation’ Comes for Okinawa,” *Diplomat*, March 20, 2025, <https://thedi diplomat.com/2025/03/chinas-malinformation-comes-for-okinawa/>.
 34. “Responding to Integrated Information Warfare With Special Regard to the Cognitive Dimension,” Japan Ministry of Defense, last visited February 5, 2026, https://www.mod.go.jp/en/d_architecture/infowarfare/index.html.
 35. “Existing Practices against Disinformation (EPaD),” Japan Ministry of Internal Affairs and Communications, 2023, https://www.soumu.go.jp/main_content/000905620.pdf.
 36. “Countering Foreign Information Manipulation and Interference (FIMI),” Ministry of Foreign Affairs of Japan, 2025, https://www.mofa.go.jp/policy/pagewe_000001_00052.html.

front activities.³⁷ Media literacy promotion and fact checking work remain heavily government led, and a genuinely whole of society mechanism involving businesses, media, academia, and civil society has yet to take shape.³⁸ This leaves Japan with a clear pattern in the information environment. Strategic coordination and international cooperation are relatively strong but domestic legal capacity and grassroots societal defense remain weaker.

Taiwan

Proximity and isolation anxiety give Beijing its entry points

Taiwan has close ties to China across history, ethnicity, religion, and the economy, and this closeness leaves room for complexity in how Taiwanese society views cross-strait policy, giving Beijing multiple points of narrative leverage with which to work. Combined with a highly diverse and politically fragmented media environment, these ties mean that narratives favorable to Beijing can usually find some outlet in Taiwan willing to carry them.

As an island that depends heavily on external trade, as well as energy and security cooperation, Taiwan carries isolation anxiety toward defense and security issues. This structural dependence creates a psychological vulnerability in which questions about whether allies and partners will truly come to Taiwan's aid remain a persistent and sensitive concern.

Taiwan's National Security Bureau has identified four main goals behind the CCP's cognitive warfare against the island: deepening internal divisions, weakening public resolve to resist, discouraging allied support, and building international sympathy for Beijing's position. To advance these goals, Beijing frequently relies on narratives questioning the reliability of the United States, the professionalism of Taiwan's military, and the legitimacy of the Lai Ching-Te administration.³⁹

Building on these existing ties, the CCP has deployed more than one hundred and fifty united front proxy networks reaching into grassroots communities and religious circles,

turning long-standing interpersonal channels into nodes for developing and reinforcing narratives of social contradiction.⁴⁰

In the digital and intelligence domains, the CCP uses civilian AI technologies such as GoLaxy to collect data and precisely microtarget audiences, while mobilizing public relations firms to proactively develop inflammatory and controversial messages. Leaked documents reveal that GoLaxy built a knowledge graph mapping Taiwanese political parties and figures across the political spectrum, classifying them by their perceived stances toward China to identify exploitable divides, and separately profiled more than thirteen thousand religious organizations and nearly twenty-four thousand civic groups.⁴¹ Beijing also distributes these messages through content farms and traditional media outlets it has long funded, giving tailored narratives ready-made channels into Taiwan's information environment.

Beijing also relies on legal warfare tools such as the Anti-Secession Law to assert legitimacy over its claims and to intimidate specific individuals, recently issuing arrest warrants targeting Taiwanese military and government personnel.⁴²

Together, this physical, digital, and legal infrastructure allows the CCP to probe for weak points and reaction thresholds and to expand its narrative database during peacetime, positioning it for rapid mobilization when a crisis provides a trigger.

Justice Mission-2025: Turning military pressure into a cognitive attack

At the end of 2025, the PLA conducted its Justice Mission-2025 exercise around Taiwan. Alongside combat readiness activities, the exercise incorporated political and propaganda elements intended to shape perceptions of the operation and its political purpose.⁴³

The first line of attack framed the exercise as legitimate and unavoidable. State media, military media accounts, and the China Coast Guard portrayed the operation as a justice-based punishment of Taiwan independence and as an exercise of law-enforcement authority. This framing recast coercive military activity as lawful punishment rather than unilateral escalation.

37. Maiko Ichihara and Tetsuro Kobayashi, "Japan's Accidental Resilience in the Disinformation Age," *Japan Times*, May 9, 2024, <https://www.japantimes.co.jp/commentary/2024/05/09/japan/japan-disinformation-age/>.

38. Kyoko Kuwahara, "Japan Must Reboot Its Disinformation Defences," *East Asia Forum*, May 24, 2025, <https://eastasiaforum.org/2025/05/24/japan-must-reboot-its-disinformation-defences/>.

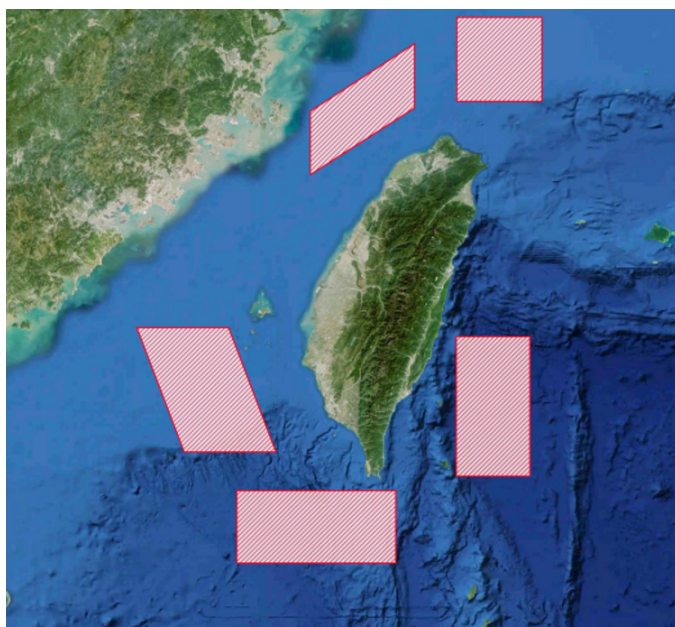
39. "Analysis of China's Cognitive Warfare Tactics against Taiwan in 2025."

40. Peter Mattis, "Stand with Taiwan: Countering the PRC's Political Warfare and Transnational Repression," hearing before the Congressional-Executive Commission on China, US Congress, July 23, 2025, https://chrissmith.house.gov/uploadedfiles/2025-07-23_peter_mattis_testimony.pdf.

41. Keoni Everington, "Chinese Database Targeting Taiwanese Politicians Leaked," *Taiwan News*, March 18, 2026, <https://www.taiwannews.com.tw/news/6323012>.

42. KaiChieh KJ Hsu, "The CCP's Legal Warfare Against Taiwan's Democracy," *Lawfare*, August 10, 2025, <https://www.lawfaremedia.org/article/the-ccp-s-legal-warfare-against-taiwan-s-democracy>.

43. John Dotson, "The PLA's 'Justice Mission-2025' Exercise Around Taiwan," *Global Taiwan Institute*, January 2, 2026, <https://global-taiwan.org/2026/01/pla-justice-mission-2025/>.



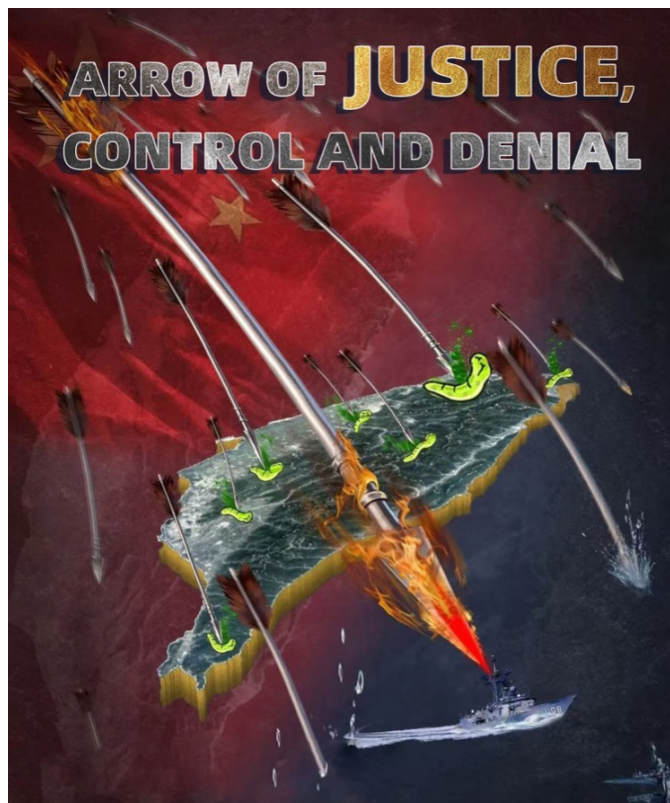
Areas of the PLA Justice Mission-2025 exercise. Credit: PLA Eastern Theater Command.

Images of PLA and Coast Guard forces emphasized China's ability to suppress Taiwan's defenses, impose a blockade, and deter outside intervention.

A second line of attack made isolation appear immediate. To demonstrate its cross-domain unmanned vehicle combat capabilities, the Eastern Theater Command utilized AI-generated imagery for the first time.⁴⁴ At the same time, Chinese media circulated fake aerial footage claiming to show a PLA drone approaching Taipei 101, while the China Coast Guard and the *Global Times* falsely claimed that Chinese vessels had blockaded Taiwan's four major ports.⁴⁵ By combining real military activity with AI-generated content and false blockade claims set in familiar Taiwanese locations, the campaign sought to make the threat of encirclement and isolation appear immediate to Taiwan's public.

The final line of attack extended the exercise into Taiwan's domestic information environment. Taiwan's National Security

Bureau recorded more than nineteen thousand controversial messages and 799 abnormal accounts on major social media platforms during the exercise.⁴⁶ Malign messaging included false claims that the defense minister was on leave alongside messaging that sought to convert travelers' inconvenience into public dissatisfaction with the government.⁴⁷ By mobilizing extensive information assets to spread false and mixed-content narratives, the campaign sought to erode trust in Taiwan's government and deepen existing political divisions, turning military pressure into a broader challenge to social cohesion and crisis management.



An "Arrow of Justice" poster released by the PLA Eastern Theater Command for the Justice Mission-2025 exercise, depicting strikes aimed at specific political groups and Taiwan's foreign helpers. Credit: PLA Eastern Theater Command.

44. PLA Eastern Theater Command (user ID 7483054836), "Joint Operations to Thwart 'Taiwan Independence' Attempts," Weibo, December 29, 2025, 1:00 a.m., <https://weibo.com/7483054836/5249190603263525>.
45. "Chinese Media Tout Drone Footage Allegedly Showing Taipei 101; MND Says UAVs Did Not Cross 24-Nautical-Mile Line," Public Television Service (PTS) News Network, December 30, 2025, <https://news.pts.org.tw/article/788333>; Chiu Shao-An, "Taiwan's Major Ports Were Not Blockaded by the Chinese Coast Guard During PLA Exercises," Taiwan FactCheck Center, December 31, 2025, <https://tfc-taiwan.org.tw/fact-check-reports/taiwan-ports-not-blockaded-by-chinese-coast-guard>.
46. Yu Kai Hsiang, "Taiwan's National Security Bureau: PLA Drills Generated 19,000 Pieces of Controversial Information and 2.09 Million Cyberattacks," Central News Agency, January 6, 2026, <https://www.cna.com.tw/news/aip/202601060164.aspx>.
47. Yao Ju Yang and Kai Hsiang Yu, "Rumors Claim Defense Minister on Leave; MND Says Chiu Li Hsiung Fully Directs Response to PLA Drills," Central News Agency, December 30, 2025, <https://www.cna.com.tw/news/aip/202512300307.aspx>; "Flight Disruption Was Deliberate Ploy, Experts Say," *Taipei Times*, January 3, 2026, <https://www.taipeitimes.com/News/taiwan/archives/2026/01/03/2003849978>.



The China Coast Guard and the state-run Global Times jointly released propaganda posters for the first time, depicting a blockade of Taiwan. Credit: China Coast Guard/Global Times.

Strong at home, constrained abroad: Taiwan's cognitive warfare defense gap

Taiwan was an early mover in responding to CCP cognitive warfare. Drawing on its shared language and cultural proximity to China, it has developed a relatively mature and organically decentralized public-private defense ecosystem. At the official level, the Executive Yuan has operated an immediate clarification mechanism since 2019, requiring ministries and agencies to actively identify false information within their areas of responsibility, verify it, and publish clarifications through official channels within four hours. The National Security Bureau routinely monitors anomalous information activity to provide early warning and supports the Executive Yuan's cross-ministerial clarification mechanism. The government also cooperates with civil society fact-checking organizations by providing official raw data for verification and using LINE, Taiwan's most widely used messaging platform, to circulate verified information to the public. Meanwhile, the Ministry of Justice Investigation Bureau has established a dedicated

Cognitive Warfare Research Center to conduct tracing analysis and proactive disclosure, strengthening official threat research capacity.⁴⁸ At the educational level, government agencies and civil society organizations have long promoted media literacy to strengthen public preparedness. The military follows the principles of taking the initiative and active countering, coordinates with the Executive Yuan to address information operations, and uses All-Out Defense Education activities to counter the CCP's physical united front threats. During crises, it also seeks greater media visibility.⁴⁹ This public-private defense ecosystem demonstrates particular strengths in education, fact checking, and research.⁵⁰

For example, during the Justice Mission-2025 military exercises, Taiwan's military proactively released monitoring footage and objective data to deliver counter-messages against CCP narratives. It provided this information to civilian fact-checking organizations and media, helping to reduce the visibility and circulation of CCP narratives in Taiwan's domestic information environment. Through information disclosure and

48. Hsieh Hsing-En, "To Counter Foreign Forces, Bureau of Investigation Establishes Cognitive Warfare Research Center," Central News Agency, January 18, 2024, <https://www.cna.com.tw/news/asoc/202401180173.aspx>.

49. "ROC National Defense Report 2025," Taiwan Ministry of National Defense, 2025, <https://www.mnd.gov.tw/newupload/ndr/114/114ndreng.pdf>.

50. Kai-Shen Huang and Muyi Chou, "Resilience in Truth: Public-Private Collaboration in Taiwan's Response to Disinformation," Research Institute for Democracy, Society and Emerging Technology, April 14, 2025, <https://dset.tw/en/research/resilience-in-truth-public-private-collaboration-in-taiwans-response-to-disinformation>.

verification, Taiwan's military reinforces societal resilience and helps disrupt and degrade the CCP's capacity to manipulate public opinion.

However, despite having social resilience, Taiwan's democratic society must balance the protection of free speech with the need for cognitive warfare defense. Taiwan lacks a foreign agents registration system and has limited compulsory regulatory power over digital platforms. Outside election periods, the government's ability to regulate malicious information or compel its removal is limited, leaving it largely reliant on self-regulation by platforms or individuals.⁵¹ These gaps are significant because some neighborhood representatives join united front-subsidized China tours, while questions persist about the funding of some temples in Taiwan.⁵² Taiwan also lacks an overarching cross-ministerial coordinating mechanism. This can lead to conflicts in resource allocation and task division, while agencies might communicate independently and weaken the overall effect of government messaging. As a result, Taiwan's bottom-up resilience remains a major strength but incomplete coordination and uneven societal coverage leave internal vulnerabilities that the CCP can exploit.

In addition, diplomatic isolation constrains Taiwan's ability to shape international narratives, creating a gap between strong domestic defenses and limited external reach. The Center for Strategic and International Studies identifies a deficit in knowledge about Taiwan's history, legal status, and cross-strait relations among global publics and political elites. This gives Beijing greater space to shape and manipulate international narratives and to limit Taiwan's participation in international forums.⁵³ Taiwan's ability to communicate counternarratives internationally is therefore constrained. During the Justice Mission-2025 exercises, the Ministry of National Defense released monitoring footage and objective information, while civil society organizations conducted fact checking. Yet Taiwan still depended on foreign governments and international media to amplify its messages abroad. This vulnerability was evident when US President Donald Trump said he was "not worried" about the exercises and had a very good relationship with Xi Jinping.⁵⁴ Without an effective international network for strategic communication, Taiwan will struggle to retain the initiative in international messaging.

Taiwan and Japan face different cognitive warfare gaps but can offset each other

The CCP uses military scenarios to activate narratives about alliance confidence, the cost of war, and internal division. Taiwan is stronger in domestic public-private defense, while Japan is better placed to work with allies and shape international messaging. This section identifies their vulnerabilities and areas for cooperation.

Democracies cannot match authoritarians' speed, but transparency can reduce the gap

Democratic societies face common vulnerabilities in information operations. Regulations often cannot keep pace with the technologies and tactics used to spread disinformation. In polarized environments, fact checking can also be portrayed

as ideological bias or censorship, weakening public trust in defensive measures.⁵⁵

Taiwan and Japan therefore face limits in responding to cognitive warfare. In Japan, the legacy of postwar militarism has made segments of the public highly sensitive to speech regulation and national security legislation, constraining legal tools for countering disinformation and improving foreign influence transparency. Taiwan has a stronger public-private defense ecosystem, but public concerns about government overreach also limit content regulation. Its proposed Digital Intermediary Services Act failed in 2022 amid concerns about privacy and government power. This creates a

51. Ibid.

52. "Taiwan POWER: A Model for Foreign Information Manipulation & Interference Resilience," Doublethink Lab, August 9, 2024, <https://medium.com/doublethinklab/taiwan-power-a-model-for-resilience-to-foreign-information-manipulation-interference-70ea81f859b7>.

53. Jude Blanchette, Ryan Hass, and Lily McElwee, "Building International Support for Taiwan," Center for Strategic and International Studies, February 13, 2024, <https://www.csis.org/analysis/building-international-support-taiwan>.

54. Jennifer Jett and Peter Guo, "China Fires a Warning to the U.S. and Simulates Taiwan Blockade, Though Trump Says He's 'Not Worried,'" NBC News, December 30, 2025, <https://www.nbcnews.com/world/asia/china-military-exercises-pla-taiwan-blockade-trump-xi-justice-mission-rcna251464>.

55. Julia Puczynska and Youcef Djenouri, "AI in Disinformation Detection," *ACIG Journal* 3, 2 (2024), <https://www.acigjournal.com/AI-in-Disinformation-Detection,200200,0,2.html>.

legal asymmetry. Authoritarian systems can coordinate resources and technology with fewer legal constraints, while democracies must balance security, free speech, trust, and political consensus. As a result, neither Taiwan nor Japan can yet raise the costs of CCP cognitive warfare campaigns enough, through domestic legal tools alone, to create credible deterrence.

The response should not be greater censorship. Democracies should focus on transparency, disclosure, and verification, including foreign funding disclosure requirements and clear labels for verified manipulated content. These measures can support civil society fact checkers, strengthen citizens' right to know, and disrupt the spread of hostile narratives—degrading the CCP's capacity to manipulate public opinion without restricting freedom of choice. They can also raise the cost of each CCP campaign. Disclosure and labeling force Beijing to rebuild exposed assets, such as the more than two hundred domains Google has blocked for targeting Japanese audiences. Shared detection across the first island chain prevents the same investment from being reused, and a decentralized verification network means the CCP must outpace many independent actors rather than persuade a single government.

Taiwan's domestic resilience and Japan's international reach create complementarity

Japan's strengths lie in strategic planning, cross-ministerial intelligence integration, and international strategic communication. Its main weakness is limited domestic civilian participation. Taiwan has stronger civilian resilience and more decentralized capacity for information disclosure and verification, but it lacks an effective official coordinating body and has limited channels to shape international narratives. Japan's domestic defense and Taiwan's external communication remain incomplete, creating clear opportunities for cooperation.

Because Taiwan is the frontline testing ground for CCP cognitive warfare, attack patterns applied there might be replicated in other countries. Taiwan has accumulated experience in identifying and responding to recurring attack patterns, and its awareness and investigation of united front activities are relatively mature. Therefore, it can share early warning indicators, analytical capacity, and government-civil society cooperating experience with Japan, improving Japan's ability to monitor threats before a crisis. Conversely, Japan can share experience in intelligence integration and cross-ministerial coordination to help Taiwan strengthen its own coordination mechanisms. Japan can also use its international communication capacity to reduce the impact of Taiwan's restricted external channels.

During military exercises or other crises, Japan should frame its public messaging around democratic values, regional maritime and air security, and developments involving PLA activities near Japan. This approach can demonstrate regional concern without issuing direct declarations of military support. It can also counter CCP narratives of unstoppable power, allied isolation, and Taiwan's abandonment.

Limits of a purely bilateral response: The case of US skepticism

Across Taiwan and Japan, the CCP uses military cognitive warfare narratives to question allied support and security cooperation, treating their disruption as a core operational objective. It repeatedly targets perceptions of US regional presence, security commitments, and support for Taiwan. In Japan's information environment, the CCP amplifies concerns over US bases in Okinawa, the risk of becoming a frontline, and the economic costs of security policies. Such narratives seek to reinforce the claim that cooperation between Tokyo and Washington threatens Japan's economy and security. When such narratives reinforce local opposition, they can raise the costs of maintaining, using, or adjusting US bases and force posture in Okinawa. This pressure can complicate US frontline response options in the Western Pacific. Meanwhile, Taiwan faces CCP narratives on arms sales and US military assistance, including claims that Taiwan is relying on the United States to seek independence and that the US will abandon Taiwan.⁵⁶

In Taiwan and Japan, long-standing defense debates allow US skepticism narratives to deepen political divisions when tied to security issues. Official clarification by either country or the United States might be absorbed into partisan debate and dismissed as political propaganda. This demonstrates the limits of a purely bilateral response in the cognitive domain. Regional partners facing similar operations can contribute detection data, platform indicators, and public assessments. Cross-validating evidence can reduce reliance on a single bilateral narrative and challenge false choices between security cooperation and domestic welfare. Yet not every criticism of US policy should be treated as malign influence. Multilateral mechanisms should give domestic audiences access to verifiable evidence and diverse regional perspectives, making it harder for coordinated manipulation to exploit political disagreement and impose binary choices.

56. "Analysis of China's Cognitive Warfare Tactics against Taiwan in 2025"; "Several U.S. Weapons Will Not Alter Inevitable Demise of 'Taiwan Independence': Spokesperson," Xinhua, March 9, 2025, <https://english.news.cn/20250309/30130326a9ed462b9b3d7e1d52708a61/c.html>.

Conclusion and recommendations

Taiwan–Japan cooperation holds clear potential but is constrained by the absence of formal diplomatic relations and the limits of the bilateral model. These two governments and that of the United States should therefore anchor cooperation within the existing multilateral security frameworks of the Indo-Pacific. As the region’s key security stakeholder, the United States has the alliance network and strategic communication reach to connect the democracies of the first island chain. The US National Defense Authorization Act (NDAA) for Fiscal Year 2026 already directs the Department of Defense to define cognitive warfare and assess the value of “narrative intelligence,” showing that Washington is building the legal basis for this mission.⁵⁷ This report therefore recommends a multilateral cognitive warfare defense network focusing on the following three lines of effort.

USPACOM should anchor a first island chain common operational picture for cognitive warfare

Cognitive warfare entails a cost asymmetry because attacks are cheap to launch while defenders bear heavy evaluation and coordination costs.⁵⁸ To lower these costs, USPACOM should lead a first island chain common operational picture (COP) for cognitive warfare, pooling each country’s monitoring capabilities into a shared transnational database. Taiwan, as the main testing ground for CCP tactics, should contribute threat cases regularly so that allies can move from reacting after the fact to early warning before a crisis. The platform would work as a narrative intelligence hub, giving planners a common view of adversary narratives and their effects and helping them prioritize defensive resources.

Table 1: Recommendations at a glance

Who acts	What, through which mechanism	Operational effect	Gap closed (see Appendix B.2)
USPACOM	Lead a first island chain common operational picture, pooling each country’s monitoring data through the III Marine Expeditionary Force (III MEF) Information Group and the Theater Information Advantage Detachment (TIAD).	Allies move from reacting after the fact to early warning before a crisis.	This compensates for both countries’ deny (D02) gap by acting at the detect (D01) stage where democracies act fastest.
Taipei and Tokyo	Supply objective data to the shared database under peace-time pre-delegation rules; civil society verifies and carries the message.	Credible third parties compress CCP narrative space among undecided audiences.	This addresses Japan’s weak civic verification (M001, M011), Taiwan’s constrained international counter-messaging (D04), and the missing coordination mechanism.
First island chain partners	Add cognitive warfare as a dedicated subject in RIMPAC and bilateral drills, from command post exercises (CPX) to live exercises (LIVEX).	Trained, coordinated, and fast allied responses become visible to Beijing.	This addresses both countries’ deter (D07) gap, which censorship-based tools cannot fill.

Note: These recommendations do not close the deny (D02) gap in law enforcement, which is left to domestic transparency legislation rather than censorship.

57. United States Senate Committee on Armed Services, “National Defense Authorization Act for Fiscal Year 2026,” S. Rep. No. 119-39 (2025), <https://www.congress.gov/committee-report/119th-congress/senate-report/39>.
58. Sara Russo, “Cognitive Warfare Is Cheap—and That’s the Problem,” Irregular Warfare Initiative, February 24, 2026, <https://irregularwarfare.org/articles/cognitive-warfare-costs-economic-asymmetry/>.

To build the COP, participating governments should agree in peacetime on shared strategic goals, narrative intelligence requirements, and specific monitoring indicators. During crises such as CCP exercises, the network should provide real-time local opinion data from officials, media, and the public so that decision-makers can identify information gaps and societal vulnerabilities and adjust their responses. The United States does not need to build this capability from scratch. The III MEF Information Group and US Army Pacific's TIAD already operate information capabilities in the region and can serve as the network's initial nodes. This arrangement strengthens detection and early warning—the response area in which democracies can act fastest—and offsets the legal limits that keep them from denying or deterring hostile campaigns at home.

Taipei and Tokyo should supply the data and let civil society carry the message

When the CCP pushes narratives such as US skepticism or abandonment, it targets the isolation anxiety shared by Taiwan and Japan as island societies. Official clarification alone rarely works. Government statements are easily dismissed as political propaganda or absorbed into partisan debate. The defense network should therefore bring in civil society, using the decentralized strengths of democratic systems to empower civilian actors. This approach can also help countries with weaker civilian fact-checking capacity, such as Japan, develop their own public-private systems. Conversely, Japan should share its cross-ministerial coordination experience to help Taiwan build an official coordinating mechanism.

The key rule is that governments and militaries act only as suppliers of objective data. Authorities must not direct civilian organizations or media in messaging. Instead, agencies should upload releasable data to the shared database for independent verification by domestic and international fact checkers. Allies can add radar or maritime monitoring data to break closed information spaces. For example, during PLA exercises, Japanese official or civilian institutions could state, based on shared data, that surrounding waters remain open, refuting blockade narratives without entering political disputes. To make this work, participating governments should set pre-delegation rules in peacetime that specify which data can be shared and when sharing begins. When credible third parties expose concrete signs of manipulation, the CCP loses narrative space among the undecided audiences it values most.

First island chain partners should train cognitive defense together in multilateral exercises

The CCP tightly coordinates its information operations with physical military pressure. Defenders must therefore train the same synchronization. The United States, Japan, Taiwan, and other first island chain partners should train cognitive defense together, adding cognitive warfare as a dedicated subject to multinational exercises such as the Rim of the Pacific (RIMPAC) and routine bilateral drills.

In the planning phase, exercise designers should draw on real threat cases accumulated in the shared database and on Taiwan's Red Team knowledge of CCP tactics to build realistic scenarios. CPX should train personnel to respond and to judge when a physical action is required, such as deploying naval vessels to counter a blockade narrative. The LIVEX phase should test transnational communication processes and mechanisms. After the exercise, participating governments should run internal communication drills with their own agencies and civil society organizations to consolidate lessons learned.

Holding such exercises is itself a deterrent signal. Democracies cannot deter cognitive warfare through censorship or content takedowns, but they can show Beijing that allied responses are trained, coordinated, and fast. These exercises also build habits of coordination among transnational stakeholders and feed back into strategic planning.

Conclusion: Standardize the language, adopt AI, outpace the threat

The network's members will work across three languages and different institutional cultures, so the shared database needs a single coding standard. DISARM already serves as a standardized schema for characterizing FIMI incidents among European and NATO practitioners. A common standard lets analysts in Taipei, Tokyo, and Honolulu describe the same campaign in the same terms, reducing interpretive drift and speeding up joint assessment.⁵⁹

AI is intensifying the threat but also works for the defense. AI agents can monitor the information environment around the clock, code incidents into the shared database, and hand the results to human analysts for qualitative judgment. Machines should run the observe and orient phases of the OODA (observe, orient, decide, act) loop, with humans keeping decide and act. This human-machine teaming attacks the cost asymmetry that favors the attacker, making defense cheaper and network-scale cooperation practical.⁶⁰

59. Kevin Tseng, et al., "An Agentic Operationalization of DISARM for FIMI Investigation on Social Media," arXiv, January 21, 2026, <https://arxiv.org/html/2601.15109v1>.

60. James Giordano, "Cognitive Warfare 2026: NATO's Chief Scientist Report as Sentinel Call for Operational Readiness," Institute for National Strategic Studies, National Defense University, January 6, 2026, <https://inss.ndu.edu/Media/News/Article/4371195/cognitive-warfare-2026-natos-chief-scientist-report-as-sentinel-call-for-operat/>.

Retired US Air Force General Mike Minihan put the stakes plainly in a 2026 Atlantic Council interview: “When you’re scared to take action because of what the enemy might do or might say, you’re being deterred.”⁶¹ Cognitive warfare is no longer a single-nation problem. The first island chain democracies

should act now, using the open and diverse nature of their societies to defend a free and truthful information space together.

Appendix A. DISARM framework overview

Red Team		Blue Team
Phase	Tactics	
Plan	TA01: Plan strategy	Response types • D01 detect • D02 deny • D03 disrupt • D04 degrade • D05 deceive • D06 destroy • D07 deter
	TA02: Plan objectives	
	TA13: Target audience analysis	
Prepare	TA14: Develop narratives	
	TA06: Develop content	
	TA15: Establish social assets	
	TA16: Establish legitimacy	
	TA05: Microtarget	
Execute	TA07: Select channels and affordances	Meta techniques • M001 resilience • M002 diversion • M003 daylight • M004 friction • M005 removal • M006 scoring • M007 meta technique • M008 data pollution • M009 dilution • M010 counter-messaging • M011 verification • M012 cleaning • M013 targeting • M014 reduce resources
	TA08: Conduct pump priming	
	TA09: Deliver content	
	TA17: Maximize exposure	
	TA18: Drive online harms	
	TA10: Drive offline activity	
	TA11: Persist in the information environment	
Assess	TA12: Assess effectiveness	

Source: DISARM Foundation, DISARM red and blue frameworks.

61. Atlantic Council, “He predicted war with China in 2025. Now Retired Gen. Minihan discusses why it hasn’t happened—yet,” YouTube, February 11, 2026, 20:41, <https://www.youtube.com/watch?v=r4nQrmtll1U&t=1241s>.

Appendix B. CCP cognitive warfare against Japan and Taiwan: Red actions and blue capabilities

B.1 CCP red framework: Japan and Taiwan compared

Country	Target audience	CCP tactic	Observed case
Plan			
Japan	Okinawa residents; general public	Target audience analysis (TA13); plan objectives (TA02)	- Sixty-eight percent see China as the primary threat, yet the public splits over intervention and the defense budget. - Eighty-five percent of Okinawans fear the island becoming a battlefield again.
Taiwan	General public; allies; international observers	Plan strategy (TA01); plan objectives (TA02)	- National Security Bureau (NSB)-identified goals: deepen internal divisions, weaken resolve, discourage allied support, build sympathy for Beijing - Narrative axes: US reliability, military professionalism, Lai administration legitimacy
Prepare			
Japan	Okinawa communities	Establish social assets (TA15); develop narratives (TA14)	- More than sixty one-day consular events, mostly in Okinawa - About 1 million Chinese nationals mobilizable under the National Defense Mobilization Law “Undetermined status of the Ryukyus” narrative themes
Japan	News consumers	Establish legitimacy (TA16)	- Impersonated local news inside Yahoo! News Japan - More than two hundred Google-blocked domains; about two hundred fake X accounts
Taiwan	Grassroots and religious communities	Establish social assets (TA15); develop narratives (TA14)	More than one hundred and fifty united front proxy networks reinforcing social contradiction narratives
Taiwan	Individuals and civic groups	Microtarget (TA05)	- GoLaxy party spectrum knowledge graph - Thirteen thousand religious organizations and twenty-four thousand civic groups profiled
Taiwan	Media consumers	Select channels and affordances (TA07)	Content farms and long-funded traditional media as distribution channels
Taiwan	Military and government personnel	Establish legitimacy (TA16)	- Anti-Secession Law asserts legitimacy over Beijing’s claims - Arrest warrants target Taiwanese military and government personnel

Country	Target audience	CCP tactic	Observed case
Execute			
Japan	Decision-makers	Deliver content (TA09)	• Wolf warrior condemnations; Osaka consul general's "beheaded" remark • UN "enemy state clauses" lawfare
Japan	Okinawa residents	Maximize exposure (TA17)	• Travel advisory discouraging visits to Japan • More than ten thousand posts declaring "Ryukyu independence"
Japan	Allied publics	Drive online harms (TA18)	• Chinese Embassy in Australia: joint drills are "preparing for war" • State media frames Japan as reviving militarism
Taiwan	General public	Deliver content (TA09); develop content (TA06)	• "Justice"-framed punishment narrative of "Taiwan independence" • First-use AI-generated imagery; fake Taipei 101 drone footage • False claims of blockading Taiwan's four major ports
Taiwan	General public	Drive online harms (TA18)	• Nineteen thousand controversial messages and 799 abnormal accounts during the exercise • False claim that the defense minister was on leave

Source: Author's categorization using the DISARM framework, drawing on sources cited in the Japan and Taiwan case studies above.

B.2 Blue framework: Established capabilities and structural gaps

Country	Response type strengths	Meta technique strengths	Structural gaps
Japan	• Detect (D01): cross-ministerial monitoring (MOFA, MOD, CIRO) • Degrade (D04): diplomatic counter-messaging in crises • Deter (D07): multinational information warfare exercises	• Meta technique (M007): cross-ministerial integration; DIH as core node • Counter-messaging (M010): UN letters, alliance messaging	• Deny (D02): no foreign agents law, no digital governance legislation • No friction (M004), removal (M005), targeting (M013), or reduce resources (M014) • Weak civic resilience (M001) and verification (M011)
Taiwan	• Detect (D01): NSB early warning; four-hour clarification mechanism • Disrupt (D03) and degrade (D04) domestically: rapid clarification and fact checking	• Daylight (M003): footage and data release • Verification (M011): fact checkers, LINE partnership • Resilience (M001): media literacy, All-Out Defense Education	• Deny (D02) and deter (D07): no foreign agents law; limited platform regulation outside elections • No friction (M004), removal (M005), targeting (M013), or reduce resources (M014) • No cross-ministerial coordinating mechanism

Source: Author's categorization using the DISARM framework, drawing on sources cited in the Japan and Taiwan case studies above.

AUTHOR BIOGRAPHY



Yu-Hao Shen

Major Yu-Hao "Vinson" Shen is a visiting military fellow of the Indo-Pacific Security Initiative at the Atlantic Council's Scowcroft Center for Strategy and Security.

He is a political warfare officer specializing in strategic communication, psychological operations, cognitive warfare, and public affairs. He dedicates himself to exploring how Taiwan can leverage strategic communication to enhance military image, gain domestic and international support, strengthen national defense resilience, and develop psychological operations to counter potential threats. He has participated in numerous engagements in Taiwan, the United States, and other countries regarding the PRC's global malign influence operations to explore collaborative models for addressing shared threats.

Recognizing the global threat posed by authoritarian regimes in the information domain, Shen is committed to exploring transnational cooperation frameworks that can establish information operation defense networks to collectively prevent the expansion of malicious threats.

Shen graduated from the National Defense University Political Warfare College (Fu Hsing Kang College) with a bachelor's degree in journalism. He is currently pursuing a master's degree at the College of Communication, National Cheng Chi University, researching "Developing Communication Strategies for the ROC Armed Forces' Crisis Management: A Contingency Theory of Public Relations Approach."



Atlantic Council

Board of Directors

CHAIRMAN

*John F.W. Rogers

EXECUTIVE

CHAIRMAN EMERITUS

*James L. Jones

PRESIDENT AND CEO

*Frederick Kempe

EXECUTIVE VICE

CHAIRS

*Adrienne Arsht

*Stephen J. Hadley

VICE CHAIRS

*Robert J. Abernethy

*Alexander V. Mirtchev

TREASURER

*George Lund

DIRECTORS

Stephen Achilles

Elliot Ackerman

*Gina F. Adams

Timothy D. Adams

*Michael Andersson

Ilker Baburoglu

Alain Bejjani

Colleen Bell

Peter J. Beshar

*Karan Bhatia

Stephen Biegun

Linden P. Blue

Brad Bondi

John Bonsell

Philip M. Breedlove

R. Nicholas Burns

Kurt M. Campbell

David L. Caplan

Samantha A. Carl-Yoder

*Teresa Carlson

*James E. Cartwright

Christopher Cavoli

John E. Chapoton

Ahmed Charai

Melanie Chen

Michael Chertoff

George Chopivsky

Wesley K. Clark

Kellyanne Conway

*Helima Croft

Ankit N. Desai

*Lawrence Di Rita

Dante A. Disparte

Denelle Dixon

*Paula J. Dobriansky

Joseph F. Dunford, Jr.

Joseph Durso

Richard Edelman

Stuart E. Eizenstat

Mark T. Esper

Christopher W.K. Fetzner

*Michael Fisch

Alan H. Fleischmann

Jendayi E. Frazer

*Meg Gentle

Thomas H. Glocer

John B. Goodman

Sherri W. Goodman

William E. Grayson

Marcel Grisnigt

Jarosław Grzesiak

Murathan Günel

Michael V. Hayden

*Robin Hayes

Tim Holt

*Karl V. Hopkins

Kay Bailey Hutchison

Ian Ihnatowycz

Keoki Jackson

Deborah Lee James

*Joia M. Johnson

*Safi Kalo

Karen Karniol-Tambour

*Andre Kelleners

John E. Klein

Ratko Knežević

C. Jeffrey Knittel

Joseph Konzelmann

Keith J. Krach

Franklin D. Kramer

Laura Lane

Almar Latour

Yann Le Pallec

Diane Leopold

Andrew J.P. Levy

Jan M. Lodai

Douglas Lute

Jane Holl Lute

Mark Machin

Marco Margheri

Michael Margolis

Chris Marlin

William Marron

Roger R. Martella Jr.

Judith A. Miller

Dariusz Mioduski

Richard Morningstar

Georgette Mosbacher

Majida Mourad

Mary Claire Murphy

Scott Nathan

*Julia Nesheiwat

Edward J. Newberry

Franco Nuschese

Robert O'Brien

*Ahmet M. Ören

Ana I. Palacio

*Kostas Pantazopoulos

David H. Petraeus

Elizabeth Frost Pierson

*Lisa Pollina

Daniel B. Poneman

Robert Portman

Dina H. Powell

McCormick

Michael Punke

Ashraf Qazi

Laura J. Richardson

*Gary Rieschel

Charles O. Rossotti

Harry Sachinis

C. Michael Scaparrotti

*Ivan A. Schlager

Rajiv Shah

Wendy R. Sherman

Gregg Sherrill

Kris Singh

Varun Sivaram

Walter Slocombe

Christopher Smith

Clifford M. Sobel

Michael S. Steele

Richard J.A. Steele

Mary Streett

Nader Tavakoli

*Frances F. Townsend

Melanne Verveer

Tyson Voelkel

Kemba Walden

Michael F. Walsh

*Peter Weinberg

Ronald Weiser

*Al Williams

Ben Wilson

Maciej Witucki

Neal S. Wolin

Tod D. Wolters

Jenny Wood

Alan Yang

Guang Yang

Mary C. Yates

Dov S. Zakheim

HONORARY

DIRECTORS

James A. Baker, III

Robert M. Gates

James N. Mattis

Michael G. Mullen

Leon E. Panetta

William J. Perry

Condoleezza Rice

Horst Teltschik

**Executive Committee Members*

List as of May 7, 2026



The Atlantic Council is a nonpartisan organization that promotes constructive US leadership and engagement in international affairs based on the central role of the Atlantic community in meeting today's global challenges.

© 2026 The Atlantic Council of the United States. All rights reserved. No part of this publication may be reproduced or transmitted in any form or by any means without permission in writing from the Atlantic Council, except in the case of brief quotations in news articles, critical articles, or reviews. Please direct inquiries to:

Atlantic Council
1400 L Street NW, 11th Floor
Washington, DC 20005

(202) 463-7226

www.AtlanticCouncil.org