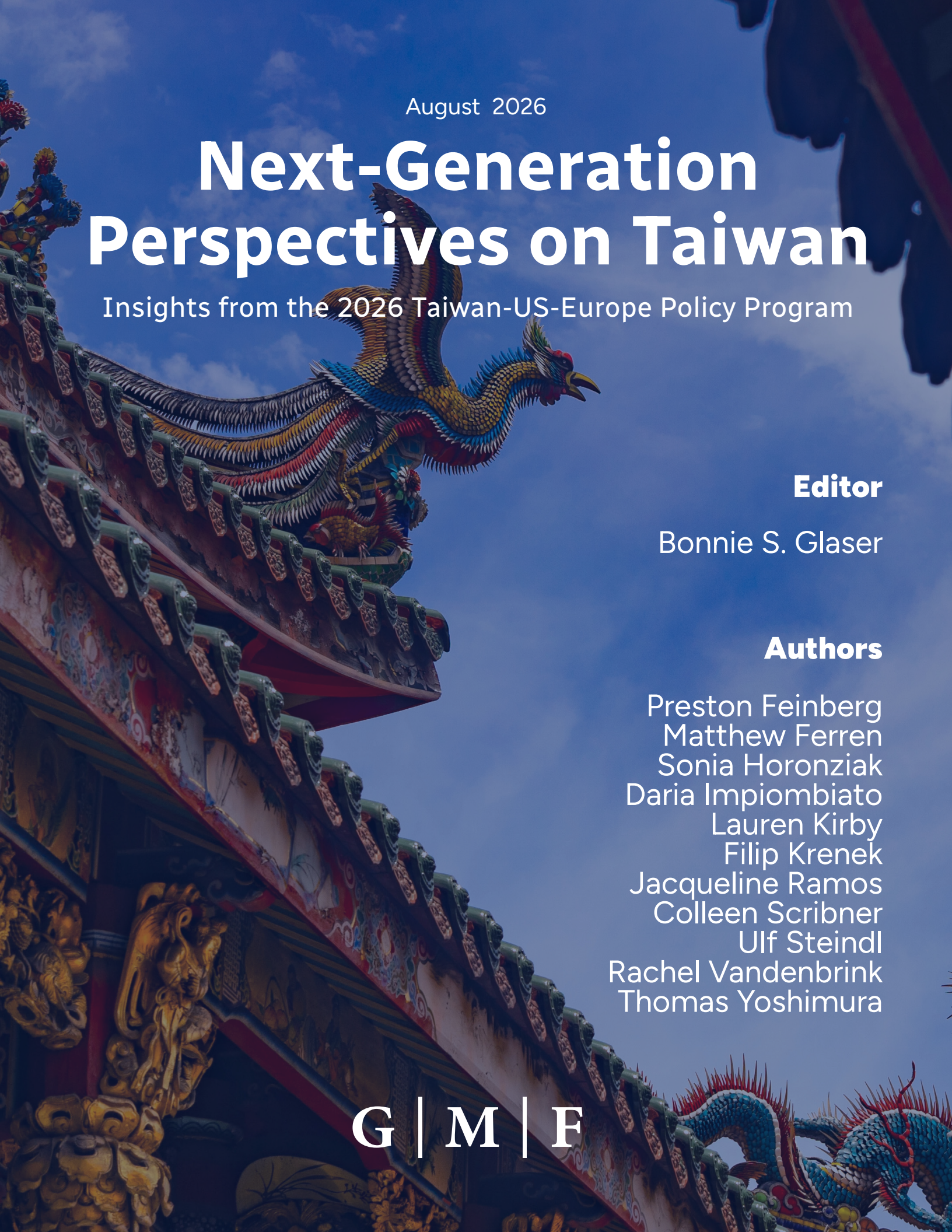




August 2026

Next-Generation Perspectives on Taiwan

Insights from the 2026 Taiwan-US-Europe Policy Program

Editor

Bonnie S. Glaser

Authors

Preston Feinberg
Matthew Ferren
Sonia Horonziak
Daria Impiombiato
Lauren Kirby
Filip Krenek
Jacqueline Ramos
Colleen Scribner
Ulf Steindl
Rachel Vandenbrink
Thomas Yoshimura

G | M | F

G | M | F

About GMF

The German Marshall Fund of the United States (GMF) is a non-partisan policy organization committed to the idea that the United States and Europe are stronger together.

Founded as an independent American foundation in 1972 by Guido Goldman (November 4, 1937 – November 30, 2020) with a gift from Germany in appreciation for aid received through the Marshall Plan after World War II, GMF is one of the world's leading international policy institutions that champions democratic values and the transatlantic alliance by strengthening civil society, forging bold and innovative policy ideas, and developing a new generation of leaders to tackle global challenges. GMF delivers hope by upholding the dignity of the individual and defending freedom in the spirit of the Marshall Plan.

GMF is headquartered in Washington, DC, with offices in Ankara, Belgrade, Berlin, Brussels, Bucharest, Paris, and Warsaw.

Disclaimer

The views expressed herein are those solely of the authors and do not necessarily reflect the policy positions of GMF or the authors' other affiliates. As a non-partisan and independent research institution, GMF is committed to research integrity and transparency.



Introduction: Next-Generation Perspectives on Taiwan4
Bonnie S. Glaser

The Chinese Military’s Cognitive Warfare Against Taiwan’s Armed Forces.....7
Preston Feinberg

Fighting Through15
Matthew Ferren

Beyond the Military22
Sonia Horonziak

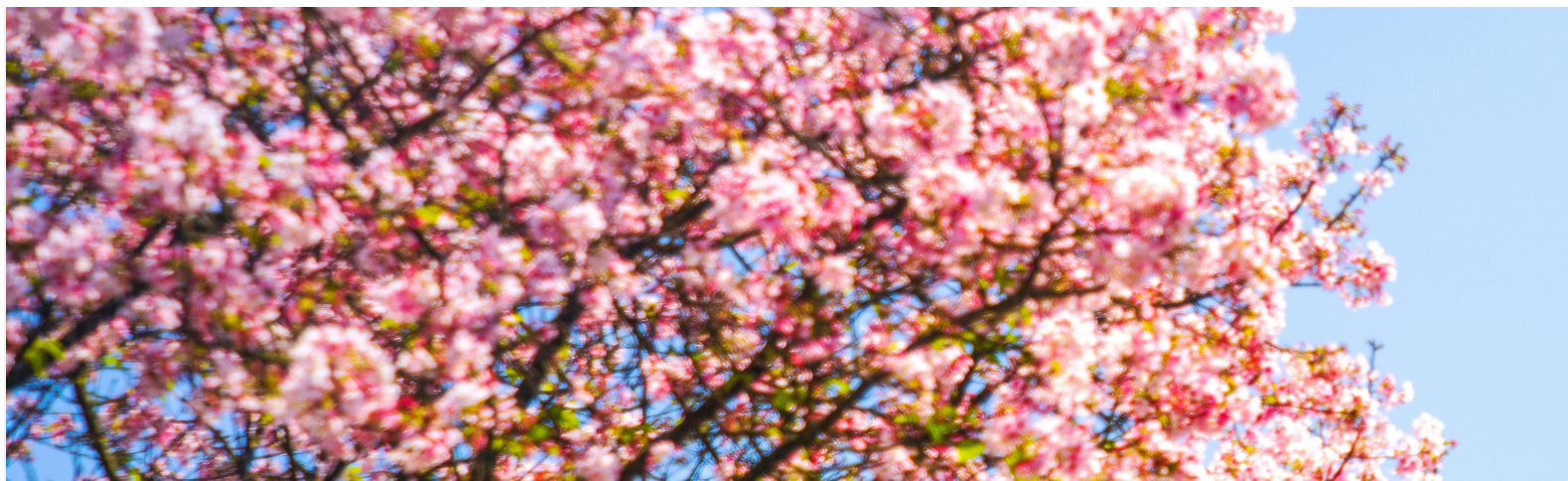
Beyond the Seven Sons29
Daria Impiombato

Civic Culture at the Heart of Taiwan’s Digital Democracy Paradox35
Lauren Kirby

From Risk to Resilience41
Filip Krenek



Preparing for Taiwan	49
Jacqueline Ramos	
Taiwan Needs an Asylum Law	56
Colleen Scribner	
Why Taiwan and the EU Should Align on Drones	62
Ulf Steindl	
Creative Workarounds	67
Rachel Vandenbrink	
The KMT, the CCP and Party-to-Party Dialogue	73
Thomas Yoshimura	
About the Authors	79



Next-Generation Perspectives on Taiwan

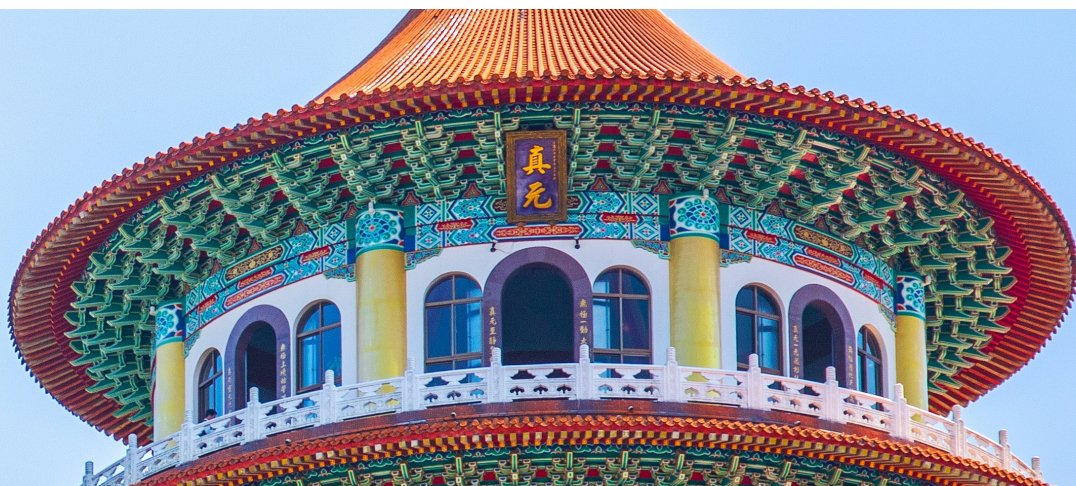
Introduction by Bonnie S. Glaser

In 2026, the People's Republic of China (PRC) made plainer than ever that it is determined to isolate Taiwan and prevent it from participating in international organizations. Its campaign extends far beyond the halls of the UN. Over the past several months alone, Beijing has reached into a World Trade Organization (WTO) ministerial, a global civil-society summit, and the airspace of three African nations to keep Taiwan off the world stage. The pattern is unmistakable: As Taiwan's democratic and economic achievements grow more visible and countries worldwide enhance their ties with Taipei, the PRC's efforts to shrink its international space grow more creative and more aggressive.

Consider the breadth of this year's record. In March, Taiwan withdrew from the WTO's 14th Ministerial Conference in Yaoundé, Cameroon, after the host government issued travel documents referring to Taiwan as "Taiwan, Province of China". That amounted to a first-ever exclusion of Taipei from a forum in which it holds full membership, and one that drew bipartisan condemnation from members of the US Congress. Two months later, the digital-rights conference RightsCon was forced to cancel its planned summit in Lusaka, Zambia, after PRC

diplomats pressured the Zambian government to bar Taiwanese civil society representatives from attending by, reportedly, leveraging Zambia's debt obligations to Beijing. In between, China pressed Madagascar, Mauritius, and the Seychelles to revoke overflight permissions for President Lai Ching-te's aircraft, forcing Taiwan's head of state to delay and then reroute a visit to Eswatini, its sole remaining diplomatic ally in Africa. Taiwan also marked its 10th consecutive year of exclusion from the World Health Assembly. The PRC is preparing to host the 2026 Asia-Pacific Economic Cooperation (APEC) forum this fall, and there are concerns it will attempt to set new terms for whether and how Taiwanese officials may take part in APEC events on Chinese soil. Each episode is different—a trade body, a human rights conference, a presidential visit, a global health forum—but together they reveal a PRC strategy that has moved well past traditional diplomatic poaching and into the granular work of denying Taiwan a seat at almost any table, public or civic, that it can reach.

None of this diminishes what Taiwan has built. It remains one of the world's most resilient democracies, having transformed itself from martial law to direct presidential elections within a single generation, and it



continues to rank among the freest societies on Earth. Its economy, anchored by a semiconductor industry that produces over 90% of the world's most advanced chips, makes it indispensable to global technology supply chains. Its public health system and its disaster-relief contributions—from earthquake aid in Japan and Türkiye to global humanitarian assistance—demonstrate a consistent ability to punch above its diplomatic weight. Taiwan is a full member of the WTO, the Asian Development Bank, and APEC, proof that it can be, and has been, a constructive and capable international partner. The gap between what Taiwan contributes and what the PRC will allow it to contribute is the defining feature of its international predicament. That gap is widening.

It is also precisely the gap that the Taiwan-US-Europe Policy Program (TUPP) was created to address. TUPP encourages young professionals from the United States and Europe to incorporate Taiwan into their research and professional work, and it helps Taiwan expand its global networks at a moment when Beijing is working overtime to constrict them. Established in 2017 and expanded in 2022 to include European participants alongside Americans—in keeping with GMF's broader mission of transatlantic cooperation—TUPP has grown into a small but durable pipeline of talent that understands Taiwan firsthand rather than through the distorted lens of Beijing's preferred narrative.

Each year, a rigorously selected cohort of 10 delegates—five Americans and five Europeans—begins the program in Washington, DC, meeting with US officials, members of Congress, and policy experts, before traveling to Taiwan for a week of direct engagement with its government, civil society, and culture. That on-the-ground exposure is the heart of the program. It is far easier to dismiss or discount efforts to isolate Taiwan from a distance; it is far harder to do so after walking its streets, sitting across the table from its officials and civic leaders, and seeing for oneself the democratic society that the PRC's pressure campaign is working to silence internationally.

Participants leave TUPP with more than an appreciation for Taiwan's history and its commitment to democratic principles. They leave with a clear-eyed understanding of just how deliberately and persistently the PRC works to deny Taiwan international standing—and of why sustained, informed engagement from the next generation of transatlantic policymakers, journalists, and researchers matters. As Beijing's tactics evolve, from courting reluctant chairs of UN bodies to pressuring debt-burdened states and rerouting presidential flight paths, the case for a broader bench of experts who know Taiwan well, and who are willing to advocate for its continued international participation, only grows stronger.

Over time, TUPP aims to build precisely that bench: a body of global experts with personal knowledge of Taiwan who will go on to support its international ties throughout their careers, whatever form they may take. It is my earnest hope that the members of this year's cohort will be inspired to work on and with Taiwan in the years ahead. I am grateful to the Henry Luce Foundation, the Global Taiwan Institute, and the Taiwan Foundation for Democracy for their continued support of this program and its goals.

The essays that follow, written by the members of the 2026 TUPP cohort, reflect the diversity of perspectives this program is designed to cultivate. I hope they prompt readers on both sides of the Atlantic to look more closely at Taiwan, and at what is at stake in the PRC's ongoing campaign to keep it off the world stage.

The Chinese Military's Cognitive Warfare Against Taiwan's Armed Forces

A threat assessment

By Preston Feinberg

The Chinese Communist Party (CCP) has long understood that the most decisive battles are not always fought with bullets and bombs. In its pursuit of unification with Taiwan, Beijing has increasingly used sophisticated and persistent forms of cognitive warfare that target the human mind rather than inflict physical harm on people or infrastructure. Cognitive warfare—the deliberate use of information manipulation and psychological operations to shape perceptions, erode morale, and undermine decision-making—has become a central pillar of the People's Liberation Army's (PLA) strategy against Taiwan's armed forces. This approach builds directly on the PLA's longstanding “Three Warfares” doctrine, which integrates public opinion warfare, psychological warfare, and legal warfare into a unified operational framework.¹ In the social media and AI era, this doctrine has evolved dramatically in scale, speed, and precision.

Taiwan's Ministry of National Defense (MND) and National Security Bureau (NSB) have explicitly described these efforts as attempts to sway the will and mindset of the island's military personnel by employing cyber tools, internet platforms, and propaganda to create confusion among troops and the broader population. The primary objective is to inspire internal subversion within the armed forces: divide loyalties, induce doubt in military leadership, undermine confidence in allied commitments—especially those of the United States—and prepare the psychological battlefield to make resistance

seem futile before a single shot is fired. As Ying-Yu Lin of Tamkang University has documented, the PLA's concept of “mind superiority” represents a deliberate doctrinal evolution designed to achieve psychological dominance over an adversary before kinetic operations begin.² This paper examines the primary mechanisms by which the PLA conducts cognitive warfare against Taiwan's military and offers considerations and recommendations for how Taipei can better protect its forces against these persistent and evolving attacks.

The Structural Vulnerability of Taiwan's Armed Forces

Before examining PLA tactics, it is worth acknowledging an underappreciated dimension of Taiwan's susceptibility to cognitive warfare: the island's force structure. Taiwan's army remains organized along Soviet-style lines, in contrast to its air force, which has been heavily influenced by American doctrine and training. The distinction matters enormously. Soviet-style organization relies on a rigid, top-down chain of command in which lower-level officers and noncommissioned officers (NCOs) execute orders rather than exercise independent judgment based on a commander's intent. This is a system of leadership known as mission command in which various echelons can make split decisions by understanding the overall commander's

objective. Research on Taiwan's military organizational culture has found that blind obedience to hierarchy can lead to impractical policies and mission failures, highlighting the deep tension between Taiwan's current command culture and the adaptive requirements of modern defense.³

This structural rigidity is a direct vulnerability in the cognitive warfare context. US Army doctrine defines "mission command" as the approach to command and control that "empowers subordinate decision-making and decentralized execution appropriate to the situation", a philosophy built on NCO initiative and trust at every echelon.⁴ Taiwan's topography, with its mountainous interior and coastal chokepoints, inherently demands decentralized, adaptive defense. Yet the army is not organized or trained to fight that way. When an adversary's cognitive operations sow confusion, spread disinformation, or create doubt about orders and leadership, a force that cannot fall back on initiative and decentralized decision-making is far more likely to hesitate, fragment, or collapse. Structural reform is therefore not merely a conventional military matter. It is a cognitive warfare countermeasure.

How the PLA Conducts Cognitive Warfare: Key Mechanisms

Disinformation and Social Media Influence Operations

Perhaps the most pervasive and scalable form of PLA cognitive warfare involves the mass dissemination of destabilizing narratives through social media platforms. TikTok, Facebook, Threads, X, and PTT (Taiwan's widely used bulletin board system) serve as primary vectors. Using networks of fake accounts, bot automation, and AI-generated content, PLA-linked actors flood the information environment with

messaging designed to erode public and military confidence. As Nathan Beauchamp-Mustafaga of the RAND Corporation has documented, the PLA's strategic support force has deployed specifically tailored social media messaging targeting PTT, with operators trained to mimic local Taiwanese dialect and sentence structure to avoid detection.⁵

The core narratives are consistent and targeted: Taiwan's armed forces are unprepared and incapable of mounting a credible defense; the United States is an unreliable partner that will ultimately abandon the island; and civilian leadership, particularly under President Lai Ching-te, is provocative and reckless. These themes are calibrated to exploit existing anxieties within Taiwanese society and the military, amplifying doubt at precisely the moments when resolve is most needed.

Critically, these operations are synchronized with PLA gray zone military activities for maximum psychological effect. During PLA military exercises in January, Taiwan's NSB documented over 19,000 such influence messages originating from 799 abnormal or bot accounts, paired with millions of cyberattacks, a deliberate effort to overwhelm digital infrastructure and psychological defenses simultaneously.⁶ Tzu-Chieh Hung and Tzu-Wei Hung, whose analysis of Taiwan's anti-disinformation experience remains among the most cited in the field, have identified four categories of Chinese cognitive operations: military intimidation, influence via bilateral exchange, religious interference, and internet-based disinformation. All were present in the January surge.⁷

The Kinmen Drone Incident: Exploitation of Embarrassment

One of the most instructive examples of PLA cognitive warfare in action occurred in August 2022, when a drone believed to have been a civilian aircraft

originating from China flew low over a Taiwanese military outpost on Kinmen Island. Footage captured two Taiwanese soldiers looking upward in apparent confusion and resorting to throwing rocks at the drone to drive it away. Beijing and PLA moved quickly, proliferating the footage across Chinese social media platforms with framing designed to portray Taiwan's forces as unprepared and incapable of defending even a small outpost. This episode exemplifies what Frank Hoffman in *Small Wars Journal* has described as the PLA's deliberate effort to shape human perception and decision-making through information manipulation, exploiting even minor incidents to construct sustained narratives of military inadequacy.⁸

Targeted Psychological Operations and Bounty Announcements

The PLA's cognitive warfare extends beyond mass messaging into targeted, individual-level intimidation. Public bounty announcements issued by China's public security bureaus, most notably from Xiamen (which faces Taiwan directly across the Taiwan Strait), have offered rewards of up to 10,000 yuan for information on specific Taiwanese military personnel, particularly those serving in psychological warfare, intelligence, and cyber units. These announcements frequently include real personal data such as names, photographs, and identification numbers, paired with accusations of separatist activities.⁹

By demonstrating that the PLA possesses detailed personal information about individual service members, these operations sow paranoia in Taiwan's armed forces. Taipei's NSB and MND have explicitly characterized these announcements as classic cognitive warfare designed to create a chilling effect by suppressing initiative, degrading internal trust, and discrediting the armed forces as infiltrated and ineffective. Edmund Burke, Kristen Gunness, Cortez A. Cooper III, and Mark Cozad, in their RAND Corporation

study of PLA operational concepts, confirm that information dominance, including dominance of psychological space, is the first and most foundational of three interlinked concepts they see as underpinning PLA doctrine in its planning over the next decade.¹⁰

Espionage, Infiltration, and United Front Recruitment

The penetration of Taiwan's military through espionage and the United Front Work Department (UFWD) recruitment represents the most corrosive form of cognitive warfare because it operates from within. The UFWD is a strategic CCP framework designed to co-opt non-party individuals and groups to support its political objectives. Its primary goal is to mobilize allies to isolate enemies, neutralize opposition, and extend the party's influence and control. To carry out its influence activities abroad, the UFWD directs "overseas Chinese work", which seeks to co-opt ethnic Chinese individuals and communities living outside China, while a number of other key affiliated organizations guided by the country's broader United Front strategy conduct influence operations targeting foreign actors and states.¹¹ Taiwan's NSB reported 48 individuals prosecuted in espionage cases in 2023 and 64 in 2024, up from just 16 in 2021. Active duty and retired military personnel account for the largest share of the accused in both years.¹² Recruitment methods range from financial inducements by targeting personnel with significant personal debt to cultural exchanges and outright coercion. The American Enterprise Institute's tracking of recent cases confirms that Chinese intelligence agents have exploited financial instability among Taiwanese military personnel, recruiting through social media and requiring recruits to film loyalty proclamations and photograph classified materials.¹³

A detailed analysis of espionage prosecutions by the Global Taiwan Institute documented one case

in which a conspiracy was uncovered to induce a special forces commander to defect by piloting a helicopter onto a Chinese aircraft carrier and other cases involving junior personnel who pledged loyalty to the PLA in videos in which they surrender.¹⁴ These examples illustrate not only the scale of penetration but the sophistication of the psychological use to which recruited personnel are put. The UFWD's role in this ecosystem extends beyond traditional espionage to include elite capture, cultural influence operations, and the long-term shaping of national identity in Taiwan, all with the aim of creating conditions conducive to eventual unification.¹⁵

Cyber-Enabled Data Exploitation and AI-Powered Targeting

According to researchers at the Institute for National Defense and Security Research (INDSR), Taiwan's governmental security think tank, the CCP conducts approximately 2.6 million cyber intrusions per day into Taiwanese systems, with healthcare, energy, and telecommunications infrastructure as primary targets.¹⁶ These intrusions are increasingly synchronized with PLA military drills, which signals active preparation for multidomain warfare rather than simple espionage. Beyond infrastructure disruption, these intrusions serve a cognitive warfare function: stealing personal and military data that enables precise targeting, supports deep-fake video production, and allows personalization of influence messaging at scale. Beauchamp-Mustafaga's analysis of generative AI's implications for PLA influence operations confirms that AI automation has dramatically lowered the cost and increased the volume of cognitive operations, with machine learning systems now capable of generating and distributing personalized disinformation at a speed no human team could match.¹⁷

Organized Crime and Religious Community Exploitation

A less publicly discussed but increasingly alarming dimension of PLA cognitive warfare involves the cultivation of potential assets within Taiwan itself. Taiwan's NSB has identified five major infiltration channels used by the CCP: organized crime groups, underground banking networks, front companies, temple organizations, and civilian associations.¹⁸ INDSR researchers have documented PLA efforts to build relationships with criminal organizations that could be activated for targeting critical infrastructure or, in extreme scenarios, political intimidation and even assassination.¹⁹ While these networks may currently serve primarily as intelligence-gathering assets, their existence represents a pre-positioned capability that could be operationalized in a crisis to amplify chaos and erode public confidence in the government's ability to maintain order.

Current Responses and Their Limitations

Taiwan has not been passive in the face of these threats. The MND has implemented programs such as "Twilight Garden", which focuses on media literacy education for troops, enhanced personnel security vetting, interagency threat mapping, and the public exposure of specific PLA operations.²⁰

However, Taiwanese officials acknowledge significant challenges. Technological asymmetry remains a serious constraint. Persistent internal political divisions, which the PLA seeks to exploit, complicate whole-of-government responses. And the aforementioned structural vulnerabilities of the armed forces mean that even the best information campaigns cannot fully offset an organizational

culture that does not support the kind of resilient, decentralized decision-making that is required for effective resistance to cognitive warfare.

Recommendations for Taiwan's Cognitive Defense

The following recommendations are designed to complement, rather than duplicate, existing initiatives. They address gaps in current doctrine, structure, and practice that have not been comprehensively addressed in existing open-source literature or policy prescriptions.

- **Establish a cognitive warfare red team within the MND.** Taiwan should create a dedicated, classified red team of military officers, psychologists, and information warfare specialists whose explicit mission is to simulate PLA cognitive operations against Taiwanese units, testing their resilience before the adversary does. Regular red team exercises should feed directly into training reforms.
- **Mandate NCO-led cognitive resilience training at the unit level.** To address the Soviet-style organizational culture that depresses NCO initiative, Taiwan should invest in a dedicated NCO cognitive warfare curriculum that empowers sergeants and staff sergeants to serve as the primary resilience vectors within their units. In degraded information environments, the NCO is the most critical decision node. Strengthening NCO capability is simultaneously a doctrinal and cognitive defense imperative.²¹
- **Create a classified debt-assistance program for military personnel.** Taiwan's NSB and the American **Enterprise Institute's** case tracking confirms that financial vulnerability is a primary recruitment vector for espionage. Taipei should consequently establish a confidential, non-punitive financial assistance program for active-duty personnel experiencing significant personal debt,²² paired with mandatory counterintelligence briefings that normalize seeking help as a patriotic act.²³
- **Develop a "cognitive inoculation" pre-deployment briefing system.** Drawing on psychological inoculation theory, the proven concept that exposing individuals to weakened forms of disinformation arguments builds resistance to stronger versions, Taiwan should develop standardized pre-deployment briefings that walk service members through the specific narratives the PLA is likely to deploy.²⁴ Jan Roozenbeek, Sander van der Linden, and colleagues demonstrated in a study of approximately 30,000 participants that pre-bunking—debunking in advance to raise awareness of mis- and disinformation—and preemptively exposing individuals to manipulative tactics produced significant improvements in their ability to identify and resist disinformation in controlled and real-world settings.²⁵
- **Partner with Taiwan's gaming industry for influence operation simulation.** Taiwan has a significant gaming and digital media sector. The MND should partner with select companies to develop immersive training simulations that place military personnel inside realistic social media influence

environments, thereby building participants' recognition of bot behavior patterns, manipulated video, and coordinated inauthentic narratives.

- **Establish a cross-strait organized crime intelligence fusion cell.** Given the documented PLA cultivation of criminal networks within Taiwan (including through religious organizations and underground banking channels identified by the NSB), the NSB, MND, and National Police Agency should create a standing fusion cell focused on mapping and monitoring the intersection of organized crime, PLA United Front activities, and potential infrastructure targeting.²⁶
- **Implement algorithmic monitoring agreements with domestic platform operators.** Taiwan should negotiate formal agreements with domestic platform operators, particularly PTT administrators and local social media companies, to share anomalous account activity data with NSB analysts in near real time during periods of elevated military tension. This would enable faster identification and disruption of coordinated inauthentic behavior before it achieves narrative saturation.
- **Develop a communication protocol for families of service members.** Cognitive operations increasingly target not just military personnel but their families, exploiting the emotional leverage that family concerns create. Taiwan should establish a secure, proactive communication protocol to keep military families informed during PLA exercises and tensions, moderating the panic and pressure that disinformation campaigns are designed to generate.
- **Formalize a “cognitive battlefield assessment” as part of after-action reviews of PLA exercises.** Following every significant PLA drill or gray-zone activity, the MND should conduct and archive a structured cognitive battlefield assessment, documenting what influence narratives were deployed, which populations were targeted, what messages achieved penetration, and how the force responded psychologically. This institutionalizes learning and builds a longitudinal database of PLA cognitive tactics.
- **Pursue a classified bilateral cognitive warfare exchange with the United States Indo-Pacific Command.** Taiwan should establish a classified bilateral working group with US Indo-Pacific Command (INDOPACOM) that focuses on cognitive warfare doctrine, threat assessment, and countermeasures. While defense cooperation already spans multiple domains, cognitive warfare remains comparatively underdeveloped within the partnership.

Conclusion

Cognitive warfare is not a peripheral concern for Taiwan's armed forces. It is a central feature of the threat environment in which they operate daily. The PLA has demonstrated consistent sophistication in its use of disinformation, targeted psychological operations, espionage, cyber exploitation, and infrastructure-linked influence efforts to erode Taiwan's military cohesion and will to resist. These operations do not pause between crises. They are persistent, adaptive, and deliberately calibrated to Taiwan's specific structural and societal vulnerabilities.

Addressing this challenge requires Taiwan to move beyond reactive countermeasures and invest in the organizational, doctrinal, and technological foundations of cognitive resilience. Empowering NCOs, closing financial vulnerability gaps, institutionalizing media literacy at the unit level, and deepening cooperation with the United States in this domain are not optional enhancements but strategic necessities. The PLA is preparing the psychological battlefield today. Taiwan must be equally deliberate in defending it.

Endnotes

¹ Ying-Yu Lin, "China's Cognitive Warfare Against Taiwan and Taiwan's Countermeasures", *Taiwan Strategists*, no. 20, 2023. <https://www.pf.org.tw/wSite/public/Attachment/003/f1702948518491.pdf>

² Ibid.

³ Chia-Shing Wu and Ji-Jen Hwang, "Reforming military organisational culture: An empirical study of the Army in Taiwan", *Defence Studies* 24, no. 4, September 12, 2024, pp. 641–665. <https://www.tandfonline.com/doi/full/10.1080/14702436.2024.2396815>

⁴ US Army, "Mission Command: Command and Control of Army Forces", Army Doctrine Publication 6-0, July 31, 2019, pp. 1–3; see also Doug Orsi and Bobby Mindell, "Will New Doctrine Fix Mission Command?", War Room, US Army War College, October 19, 2019. <https://warroom.armywarcollege.edu/articles/new-doctrine-mission-command/>

⁵ Nathan Beauchamp-Mustafaga, "Cognitive Domain Operations: The PLA's New Holistic Concept for Influence Operations", *China Brief* 19, no. 16, Jamestown, September 6, 2019. <https://jamestown.org/cognitive-domain-operations-the-plas-new-holistic-concept-for-influence-operations/>

⁶ Tzu-Chieh Hung and Tzu-Wei Hung, "How China's Cognitive Warfare Works: A Frontline Perspective of Taiwan's Anti-Disinformation Wars", *Journal of Global Security Studies* 7, no. 4, 2022. <https://academic.oup.com/jogss/article/7/4/ogac016/6647447>

⁷ Ibid.

⁸ Frank Hoffman, "Assessing 'Cognitive Warfare'", *Small Wars Journal*, November 14, 2025. <https://smallwarsjournal.com/2025/11/14/assessing-cognitive-warfare/>

⁹ Russell Hsiao, "Recent Chinese Spy Cases in Taiwan: Knowns, Unknowns, and Implications", *Global Taiwan Brief* 9, no. 17, Global Taiwan Institute, September 4, 2024. <https://globaltaiwan.org/2024/09/recent-chinese-spy-cases-in-taiwan/>

¹⁰ Edmund J. Burke, Kristen Gunness, Cortez A. Cooper III, and Mark Cozad, "People's Liberation Army Operational Concepts", RR-A394-1, RAND Corporation, 2020. https://www.rand.org/pubs/research_reports/RRA394-1.html

¹¹ U.S.-China Economic and Security Review Commission, "China's Overseas United Front Work: Background and Implications for the United States", August 24, 2018. <https://www.uscc.gov/research/chinas-overseas-united-front-work-background-and-implications-united-states>

¹² Taiwan National Security Bureau, "Annual Report on PRC Espionage Operations in Taiwan", National Security Bureau, January 12, 2025; translated summary at David Cowhig's Translation Blog, January 13, 2025. <https://gaodawei.wordpress.com/2025/01/13/2025-taiwan-national-security-bureau-on-prc-spies/>

¹³ Dan Blumenthal, et al., "China & Taiwan Update", *American Enterprise Institute and Institute for the Study of War*, April 24, 2026. <https://www.aei.org/articles/china-taiwan-update-april-24-2026/>

¹⁴ Hsiao, "Recent Chinese Spy Cases in Taiwan".

¹⁵ Interview with Pei-Shiue Hsieh, Jyh-Shyang Sheu, and Christina Chen, Institute for National Defense and Security Research, March 7, 2026.

¹⁶ Ibid.

¹⁷ Nathan Beauchamp-Mustafaga, "Exploring the Implications of Generative AI for PLA Influence Operations", CTA3191-1, RAND Corporation, February 1, 2024. https://www.rand.org/content/dam/rand/pubs/testimonies/CTA3100/CTA3191-1/RAND_CTA3191-1.pdf

¹⁸ Taiwan National Security Bureau, "Annual Report on PRC Espionage Operations in Taiwan", 2025.

¹⁹ Interview with Pei-Shiue Hsieh, Dr Jyh-Shyang Sheu, and Christina Chen, March 7, 2026.

²⁰ Republic of China Ministry of National Defense, "The P.R.C.'s Cognitive Warfare: Enemy Threats and R.O.C. Armed Forces Preparedness", excerpt from the R.O.C. National Defense Report to the 4th Session of the 11th Legislative Yuan, October 1, 2025. <https://www.mnd.gov.tw/en/publication/113>

²¹ Taiwan National Security Bureau, "Annual Report on PRC Espionage Operations in Taiwan", 2025.

²² Fred N. Tolman, "Mission Command: A Senior Enlisted Leader's Perspective", *NCO Journal*, May 2020. <https://www.armyupress.army.mil/Portals/7/nco-journal/images/2020/May/Mission-Command/mission-command.pdf>

²³ Blumenthal, et al., "China & Taiwan Update"; Taiwan National Security Bureau, "Annual Report on PRC Espionage Operations in Taiwan", 2025.

²⁴ Fred N. Tolman, "Mission Command: A Senior Enlisted Leader's Perspective", *NCO Journal*, May 2020. <https://www.armyupress.army.mil/Portals/7/nco-journal/images/2020/May/Mission-Command/mission-command.pdf>

²⁵ Jon Roozenbeek, Sander van der Linden, and Thomas Nygren, "Prebunking interventions based on the psychological theory of 'inoculation' can reduce susceptibility to misinformation across cultures", *Harvard Kennedy School Misinformation Review* 1, no. 2, 2020. <https://misinforeview.hks.harvard.edu/article/global-vaccination-badnews/>

²⁶ Taiwan National Security Bureau, "Annual Report on PRC Espionage Operations in Taiwan", 2025; Kelvin Chen, "GTI Report Highlights China's Far-Reaching Infiltration Campaign against Taiwan", *Taiwan News*, April 1, 2025. <https://www.taiwannews.com.tw/news/6074379>

Fighting Through

Cyber Resilience as a Warfighting Requirement for Taiwan

By Matthew Ferren

Taiwan lives in a dangerous digital neighborhood. In 2025, cyber threat actors linked to the People's Republic of China (PRC) attempted 2.63 million intrusions per day on Taiwan's critical infrastructure networks, as estimated by the National Security Bureau.¹ These intrusions spanned the full range of state-directed malicious cyber activity: industrial and political espionage, financially motivated cybercrime and scams, information operations, and compromise of critical infrastructure networks.² The volume, persistence, and apparent strategic intent of these operations have, understandably, made cyber resilience a central focus of Taiwanese policymakers.

Yet the cyber threat Taiwan would face in conflict differs in important ways from the one it faces today. Modern militaries are growing more adept at integrating cyber and electronic warfare into joint operations, using them to jam communications, blind sensors, and disrupt command networks. The People's Liberation Army (PLA) is investing heavily along these lines, and in conflict would direct these capabilities at the island's military networks and command systems—an additional challenge layered on top of the threat to critical infrastructure. Taiwan's cyber strategy, organized principally around cyber hygiene and civilian resilience, has not yet caught up.

Taiwan should reframe cyber resilience as a foundational warfighting requirement. Doing so requires a planning baseline grounded in the targets and effects the PLA is most likely to pursue, investments in military cyber resilience

commensurate with those in civilian infrastructure, and deeper operational integration with the United States and other partners. Together, these steps will make Taiwan's military deterrence more credible and, if deterrence fails, give its forces the ability to fight through disruption.

Taiwan's Cyber Maturation

Taiwan has made cyber resilience a strategic priority. Building on a prioritization of cyberspace that began under President Tsai Ing-wen, successive administrations have treated cybersecurity as foundational to national security and backed that framing with sustained executive attention. The April 2025 National Cybersecurity Strategy sets priorities across critical infrastructure protection, supply chain risk management, workforce development, and international cooperation.³ Phase VII of the National Cybersecurity Development Program (2025–2028) operationalizes those priorities through implementation responsibilities, measurable targets, and investments synchronized with broader digital and defense modernization efforts.⁴ Taiwan's conception of cyber resilience is expansive: Under President Lai Ching-te's Whole of Society Defense Resilience plan, technical defense of critical networks sits alongside societal resilience to PRC pressure—countering information operations, building public trust, and sustaining essential services during crises—as a single integrated problem set.

Translating that prioritization into operational capacity has required new coordination mechanisms and stronger regulatory teeth. The Ministry of Digital Affairs, established in 2022, gave Taiwan a unified civilian cybersecurity authority for the first time, and Taipei is now standing up its National Cyber Collaborative Operational Center to share intelligence and coordinate defensive operations across government and with the private sector. The September 2025 amendments to the Cybersecurity Management Act expand the scope of regulated entities, strengthen incident reporting and supply chain risk management requirements, and increase penalties for noncompliance, to address concerns that the Act's original enforcement regime was too weak to drive consistent practice across critical sectors.⁵

Military institutions have followed a parallel trajectory. The Information, Communications, and Electronic Force Command (ICEFCOM), established in 2017, leads military cyberspace operations and electronic warfare, with a growing emphasis on "active cyber defense"—offensive operations that proactively disrupt PRC cyber campaigns. How these mechanisms would scale and operate under wartime command authorities, however, remains largely untested.

Taken together, these reforms have produced a cyber posture that is stronger than it was five years ago. Taiwan is better able to detect intrusions, defend critical infrastructure, and contain disruption, and its civilian and military institutions are more clearly delineated and better resourced than at any point in its history. Inconsistent enforcement of cybersecurity standards across critical sectors, interagency coordination challenges, and persistent workforce shortages remain barriers to full implementation of Taipei's cybersecurity vision, but the civilian side of the ledger is pointed in the right direction. The harder question is whether that posture, built largely against

peacetime threats to civilian networks, is sufficient to ensure Taiwan's military readiness.

The Evolving Role of Non-Kinetic Effects

Much of the alarm in Taiwan has centered on PRC campaigns to pre-position access to power, water, telecommunications, and other critical infrastructure, which could enable Beijing to cause significant disruption of essential services in crisis. That concern is well-founded for a scenario in which Beijing seeks to paralyze Taiwan in the opening hours of an attempted full-scale invasion. But Taiwan's own defense concept points toward a prolonged conflict. The 2025 National Defense Report formalizes a strategy of "erosion": Rather than staking the island's survival on an all-or-nothing defense, Taiwan's forces would contest PLA landings while holding combat power in reserve to attrit the invading force through asymmetric operations and buy time for international intervention.⁶

Erosion is, by design, a protracted fight—and it is on that timeline that standalone cyberattacks on civilian infrastructure have proven less impactful. In Ukraine, Russian operations against electricity, telecommunications, financial services, and government systems produced isolated disruptions that defenders quickly reversed. Once existing accesses were burned, Russian operators struggled to reestablish footholds at the pace required for repeat effects.⁷ As the conflict ground on, Moscow increasingly turned to missiles and unmanned aerial systems as a more reliable means of inflicting damage to critical infrastructure.

Cyber and electronic warfare have proven more useful as enablers of joint military operations—generating

tactical intelligence, supporting targeting of logistics nodes, and disrupting command and control—than as substitutes for conventional fires. In US operations in Venezuela and Iran, cyber, space, and other non-kinetic effects have been “layered” with air strikes and special operations raids to blind enemy sensors and disable air defenses.⁸ Non-kinetic effects have contributed to tactical and operational success without proving decisive on their own.

The PLA appears to be adapting to this new paradigm. PLA doctrinal writings on “informatized” and “intelligentized” warfare emphasize the importance of disrupting an adversary’s decision cycle, degrading its ability to sense and engage, and protecting one’s own information advantage—objectives served principally by integrated cyber, electronic warfare, and information operations against military targets.⁹ The April 2024 reorganization of the former Strategic Support Force into the Aerospace Force, Cyberspace Force, and Information Support Force reflects this emphasis. The new Cyberspace Force now includes five regional Technical Reconnaissance Bases that align with the PLA’s military theaters, consolidating signals intelligence and cyber capabilities in support of theater command operations, while a separate Cyberspace Operations Base oversees strategic-level offensive cyber operations. The pairing enables the PLA to integrate non-kinetic effects with joint operations while sustaining a disruption capacity against adversary critical infrastructure and decision-making.¹⁰

In a conflict with Taiwan, PLA cyber and electronic warfare would serve three overlapping objectives. The most direct is enabling the PLA’s amphibious, missile, and air operations against the island by simultaneously degrading the Taiwan military’s operations and accelerating the PLA’s own. Cyber intrusions and electronic attack against the networks and radios that connect Taiwanese commanders to their units,

the radars and sensors that detect incoming threats, and the fire control systems on platforms such as air defenses and coastal defense missile batteries would leave units unable to coordinate, identify targets, or engage incoming forces at key moments. Concurrently, cyber espionage and signals intelligence against Taiwan’s command networks and military communications would be used to locate command posts, mobile launchers, and reserve formations for PLA strike.

The PRC would also use cyber operations to shape Taiwan’s political dynamics in crisis. Information operations—coordinated disinformation across social media, manipulated audio and video, and amplification of pro-PRC voices in Taiwanese discourse—would seek to fracture public consensus on whether Taiwan can prevail and whether the cost of resisting is worth bearing. Disruption of civilian services, particularly when timed with kinetic strikes, would make day-to-day life materially harder, raise the visible cost of conflict, and undermine government legitimacy. Sustained over a protracted erosion fight, these effects would work to reduce the will to fight on which Taiwan’s defense concept depends.

Pre-positioned access on critical infrastructure could be activated to compound those effects, in Taiwan and beyond. Disrupting US critical infrastructure and military networks—at facilities in Guam, Japan, and Hawaii, and on continental transportation and logistics nodes—would slow mobilization, complicate sustainment, and inject confusion into allied decision-making during the phase of a crisis when intervention decisions are made.¹¹

Implications for Taiwan's Defense Posture

Preparing for a cyber-enabled conflict requires Taiwan to harden its military networks and infrastructure against PRC interference; train and equip its forces to operate through degradation; and prepare to employ its own cyber and electronic warfare capabilities in close coordination with military operations in other domains. Each of these requires new doctrine, capabilities, and investment, supported by revisions to joint plans, training, and exercises. Five lines of effort merit prioritization.

- **Harden Defense Networks:** Civilian critical infrastructure has rightly received attention in recent years, but the cybersecurity of core military networks and weapons platforms—radars, coastal defenses, integrated fire control, and the Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR) backbone—should also be hardened against PRC compromise. This can be achieved through recurring hunt campaigns to detect and clear PRC prepositioning, deployment of cyber sensors and deception tools, and targeted replacement or retrofit of platforms whose vulnerabilities cannot be mitigated through patching alone.
- **Conduct Exercises Under Realistic Conditions:** Han Kuang and other major exercises have improved in recent years, but their non-kinetic dimension remains thin. Taiwanese commanders and units should plan and exercise operations that assume key C2 systems are down, communications are jammed or intermittent, Global Positioning System (GPS) tracking is denied or spoofed, radars and sensors are intermittently blinded, and certain weapons platforms are degraded. Exercises should sustain these conditions for extended periods, testing the ability of Taiwan's forces to maintain coherent joint action; lessons should be fed back into joint plans and training requirements for conventional units.
- **Adopt a Defend Forward Posture Against PRC Pre-positioning:** PRC cyber forces are actively pursuing pre-positioned access on Taiwanese and partner networks to enable disruption in conflict. ICEFCOM should adopt a "defend forward" posture—hunting and clearing ROC and partner networks, in coordination with US Cyber Command and allied services. This posture would reduce what the PRC can activate in conflict and would improve ICEFCOM readiness and partner relationships. The Ministry of National Defense (MND) should further prepare, plan for, and posture ICEFCOM to employ this capacity in crisis to defend Taiwan's networks and disrupt PLA non-kinetic effects.
- **Invest in PNT Resilience:** Position, navigation, and timing (PNT) services from US GPS underpin military operations as well as financial markets, telecommunications, and transit, representing a key cross-sector vulnerability. Taiwan routinely experiences PRC jamming and spoofing of GPS, while the PRC has reduced its own vulnerability through a national eLoran network.¹² Taiwan should pursue a layered alternative—a terrestrial low-frequency backup similar to eLoran, fiber-optic timing distribution to critical infrastructure, and integration with Japan's Quasi-Zenith Satellite System—to raise the cost of PNT denial.

- **Integrate Non-Kinetic Effects Into Joint Operational Plans:** Taiwan's cyber, electronic warfare, and Signals Intelligence (SIGINT) capabilities should be planned and exercised as enablers of the joint fight, not as a parallel campaign. ICEFCOM should align a portion of its offensive cyber and SIGINT capacity with theater fires, generating intelligence on PLA logistics, amphibious staging, and command nodes to enable targeting. MND should assess the need for adjustments to force structure and doctrine that enable employment of non-kinetic effects at the tactical level to degrade PLA amphibious and air-assault command networks, ISR platforms, and fire-control links. This requires joint targeting processes that treat non-kinetic effects as fires, authorities that allow ICEFCOM to act alongside tactical decision cycles, and regular rehearsal in exercises.

The Role of Partners

Taiwan cannot prepare for a cyber-enabled conflict alone. The United States should expand its support for Taiwan's non-kinetic development, with allied governments and private sector partners playing complementary roles, along five lines of effort.

- **Expand Cyber Exercises and Operator Integration:** Section 1518 of the US FY24 National Defense Authorization Act directs expanded cooperation on defensive cyber activities with Taiwan, but the Department of Defense has not maximized the use of these authorities. Combined cyber exercises with Taiwan remain limited in scope and frequency relative to those conducted with other Indo-Pacific partners, and the authority has not yet been used to embed US cyber operators with counterparts in Taiwan during major exercises like Han Kuang. Bilateral exercises should expand across the board and should focus on maintaining integration under degraded communications, coordinating fire and maneuver under integrated cyber and EW pressure, and performing cyber incident response and recovery.
- **Develop Joint Cyber Playbooks:** US and Taiwanese policymakers should develop joint playbooks for responding to the full spectrum of PRC cyber pressure, from gray zone espionage and pre-positioning to infrastructure disruption, information operations, and integrated cyber-kinetic effects. The Global Cooperation and Training Framework (GCTF)—a knowledge-sharing platform that includes Japan, Australia, Canada, and the United Kingdom—is a natural vehicle for accelerating these discussions and bringing in additional Indo-Pacific partners.
- **Invest in Regional Communications Resilience:** Subsea cable repair capacity in the Western Pacific is limited and slow, and sustained PRC pressure in crisis could quickly reduce Taiwan's ability to communicate with partners. Resilient Low Earth Orbit (LEO) satellite communications for Taiwan and US forces in the first island chain need deliberate planning and investment now, including service availability arrangements under crisis conditions, rather than improvisation later. Coordinating PNT alternative investments with Japan and other allies would address shared GPS dependency

risks and the asymmetry created by the PRC's eLoran deployment.

- **Clarify Private Sector Roles in Conflict:** Drawing on lessons from Ukraine, the United States and Taiwan should clarify the role of private sector providers in responding to cyber incidents in conflict. Cloud backups, satellite communications, threat intelligence, and incident response capacity—all central to sustaining Taiwanese operations—come largely from US and allied companies, yet the roles, authorities, and indemnification arrangements governing their wartime employment are largely unwritten. Working through them in advance is more efficient than discovering the gaps under operational pressure; the private sector is already starting this work, and governments should support and accelerate it.¹³
- **Engage European Partners on the Information Environment:** Years of countering Russian information operations and supporting societal resilience under sustained influence campaigns have given European governments and civil society organizations distinctive expertise on the civilian information environment. Practical assistance to Taiwan in this area—through civil society partnerships, fact-checking infrastructure, and journalist training—plays to that comparative advantage and would augment Taipei's already robust capacity in this space.

Conclusion

The credibility of Taiwan's deterrence rests on the proposition that an invasion would likely fail and that the costs of attempting one would be unacceptable to Beijing. The cyber dimension of that proposition depends less on the integrity of any single network than on the demonstrated ability of Taiwanese forces and partner formations to fight through the contested digital environment a conflict would almost certainly create. Treating cyber resilience as a warfighting requirement is what produces forces and infrastructure that can absorb disruption and keep operating. That is the standard against which the next several years of investment, training, and partnership should be measured.

Endnotes

¹ Taiwan National Security Bureau, "Analysis on China's Cyber Threats to Taiwan's Critical Infrastructure in 2025", January 4, 2026. <https://www.nsb.gov.tw/en/assets/documents/%E6%96%B0%E8%81%9E%E7%A8%BF/9976f2e1-3a8a-4fa2-9a73-b0c80fca1f04.pdf>

² Mark Kelly, "Phish and Chips: China-Aligned Espionage Actors Ramp Up Taiwan Semiconductor Industry Targeting", Proofpoint, July 16, 2025. <https://www.proofpoint.com/us/blog/threat-insight/phish-china-aligned-espionage-actors-ramp-up-taiwan-semiconductor-targeting>; Microsoft Threat Intelligence, "Flax Typhoon using legitimate software to quietly access Taiwanese organizations", August 24, 2023. <https://www.microsoft.com/en-us/security/blog/2023/08/24/flax-typhoon-using-legitimate-software-to-quietly-access-taiwanese-organizations/>; Joanna Octavia, "Online Fraud and Scams in Taiwan", Safer Internet Lab Report, CSIS Indonesia, 2025. <https://saferinternetlab.org/wp-content/uploads/2025/05/Online-Fraud-and-Scams-in-Taiwan.pdf>

³ National Security Council, "National Cybersecurity Strategy 2025: Cybersecurity is National Security", National Information & Communication Security Office, April 2025.

⁴ Eryk Waligora, "Advancing Cyber Resilience: Taiwan's Strategic Shift in the Seventh Phase of Its National Cybersecurity Program", Global Taiwan Brief 10(14), Global Taiwan Institute, July 16, 2025. <https://globaltaiwan.org/2025/07/advancing-cyber-resilience-taiwans-strategic-shift/>

⁵ Ministry of Digital Affairs, "Cyber Security Management Act", September 24, 2025. <https://law.moj.gov.tw/ENG/LawClass/LawAll.aspx?pcode=A0030297>

⁶ Ministry of National Defense, "ROC National Defense Report 2025", October 2025. <https://www.mnd.gov.tw/newupload/ndr/114/114ndreng.pdf>

⁷ Jon Bateman, "Russia's Wartime Cyber Operations in Ukraine: Military Impacts, Influences, and Implications", Carnegie Endowment for International Peace, December 16, 2022. <https://carnegieendowment.org/research/2022/12/russias-wartime-cyber-operations-in-ukraine-military-impacts-influences-and-implications>

⁸ Julian E. Barnes and Adam Sella, "How Computer Warfare Is Becoming Part of the Pentagon's Arsenal", The New York Times, January 27, 2026. <https://www.nytimes.com/2026/01/27/us/politics/pentagon-computer-warfare.html>; Martin Matishak, "Cyber Command disrupted Iranian comms, sensors, top general says", The Record, March 2, 2026. <https://therecord.media/iran-cyber-us-command-attack>

⁹ US Department of Defense, "Military and Security Developments Involving The People's Republic of China", December 18, 2024. <https://media.defense.gov/2024/Dec/18/2003615520/-1/-1/0/MILITARY-AND-SECURITY-DEVELOPMENTS-INVOLVING-THE-PEOPLES-REPUBLIC-OF-CHINA-2024.PDF>

¹⁰ John Costello, "The Cyberspace Force: A Bellwether for Conflict", China Brief 25 (8), Jamestown, April 25, 2025. <https://jamestown.org/the-cyberspace-force-a-bellwether-for-conflict/>

¹¹ Annie Fixler, Mark Montgomery, and Rory Lane, "Military Mobility Depends on Secure Critical Infrastructure", CSC 2.0, March 2025. <https://www.fdd.org/wp-content/uploads/2025/03/fdd-csc2.0-military-mobility-depends-on-secure-critical-infrastructure.pdf>

¹² John Plumb, "PNT Resilience for an Era of Great Power Competition", CSIS, October 31, 2024. <https://www.csis.org/analysis/pnt-resilience-era-great-power-competition>

¹³ Cyber Defense Assistance Collaborative, "Four Years of Cyber Assistance to Ukraine", CRDF Global, March 2026. <https://crdfglobal-cdac.org/four-years-of-cyber-assistance-to-ukraine/>

Beyond the Military

Shifting Perceptions of Civil Society's Role in National Defense in Taiwan

By Sonia Horonziak

Building societal resilience—public readiness to meet a range of challenges and threats, from natural disasters to military conflict—is becoming an increasingly prominent item on national agendas¹. Civil preparedness is gaining importance as part of countries' efforts not only to equip civilians with the knowledge and skills needed to cope collectively with crises, but also to strengthen national deterrence and defense strategies.² However, approaches to implementing whole-of-society resilience vary depending on the number of actors involved and the nature of cooperation among the state, the military, civil society organizations, and other stakeholders.

Civil society, understood as a collective of NGOs, community groups, and individuals undertaking various forms of social activity, plays a crucial role in building social resilience and crisis preparedness. To be fully effective, its role should extend beyond simply supporting government actions to include assuming responsibility for itself and others before and during crises, often even before institutional response mechanisms are activated. However, achieving this goal requires civil society be adequately supported, by the state along with other actors, financially, logistically, and informationally, while also being integrated into government activities at multiple levels.

The example of Taiwan illustrates how perceptions of civil society's role in national defense have evolved over time. Although the trajectory is in the right direction, progress does not necessarily guarantee

success. On the one hand, Taiwanese civil society has gained increasing recognition in recent years, including from government institutions; on the other hand, it continues to struggle for a stable position within the public sphere, as well as for adequate support and broader recognition of its activities. What is still missing is the permanent link—an institutionalized body that can ensure that the authorities and civil society representatives can cooperate with each other on a continuous basis. This combination would reduce the likelihood of duplication of work between these two actors and enhance the exchange of information and knowledge without an imposed top-down agenda. Its creation, however, should be part of a larger framework in which Taiwan's civil society conducts its activities and receives support at all levels of state governance, from national policies to local structures.

Where There Is Crisis, Civil Society Shines

This shift toward viewing civil society as an active agent of change rather than merely a recipient of state policy has emerged in many countries, including Taiwan, in recent years. Although efforts to strengthen societal resilience, particularly in the area of natural disaster response, have existed in Taiwan since the 2000s, a major turning point in perceptions of civil society occurred during the COVID-19 pandemic. In 2020, Taiwan's minister of the interior issued

guidelines coordinating not only official local facilities but also schools, civic groups and volunteers in efforts to combat the pandemic. This demonstrated that Taiwanese civil society was willing to undertake voluntary initiatives and act as a collaborative partner alongside national and local government authorities. At the same time, many civic organizations and human rights groups maintained their role as watchdogs over the government's actions, especially regarding potential limitations on civil liberties introduced during the crisis.³

Another major development that reshaped the Taiwan administration's appreciation of the role of civil society was Russia's full-scale invasion of Ukraine in 2022. The war demonstrated that maintaining the status quo is not always possible in the face of revisionist or imperial ambitions, while it also served as a real-time test of both state and social resilience. Humanitarian assistance provided by local communities and civil society organizations proved crucial in evacuating civilians from dangerous regions. Voluntary donations from citizens helped fund not only military equipment but also the activities of NGOs. Importantly, Ukrainian NGOs have not operated as isolated entities, but rather as overlapping and interconnected networks capable of supporting—and at times compensating for weak political institutions.⁴

The Russian invasion prompted Taiwanese society to prepare more seriously for the possibility of a large-scale and prolonged conflict, while also becoming more closely aligned with the concept of “whole-of-society resilience”. In 2022, under the administration of President Tsai Ing-wen, Taipei issued its first civil defense handbook for citizens.⁵ In addition, societal participation in national defense was emphasized in the military's Overall Defense Concept,⁶ particularly through the mobilization of civilian resources. However, the most significant shift toward

recognizing the active role of civil society from the early stages occurred after Lai Ching-te assumed the presidency in 2024.

Civil Society as a Deterrent Force?

In June 2024, only one month after taking office, President Lai established the Whole-of-Society Defense Resilience (WOSDR) Committee with himself acting as chair.⁷ Its purpose was to serve as a platform for social participation and communication between the government and society during national emergencies or natural disasters. The Committee included representatives from government institutions, industry, civil society organizations, and academia covering areas such as civilian training, critical infrastructure, supply maintenance and distribution, and social welfare. The initiative was presented as a continuation of the efforts initiated under the Tsai administration.

Although official government messaging did not explicitly emphasize the possibility of a military attack—consistent with Taiwan's long-standing strategy of avoiding overly alarmist public communication—the government's actions clearly reflected a growing focus on societal resilience as part of a broader deterrence plan.

One of the most visible and symbolically significant manifestations of Taiwan's new resilience strategy was the launch of the country's largest-ever 10-day Urban Resilience Exercises in July 2025.⁸ These exercises combined civilian air-raid preparedness measures with the annual Han Kuang military drills. Nevertheless, the 2025 format largely preserved a separation between civilian and military components, reflecting an institutional assumption that parallel but distinct

preparedness structures would be sufficient during a crisis.⁹

A notable evolution emerged during the 2026 Urban Resilience Exercises, which commenced on April 22.¹⁰ The drills mobilized alternative service personnel alongside municipal governments and integrated activities such as air-raid warning systems, evacuation procedures, and disaster-response operations. Additional exercises were subsequently planned across ten municipalities nationwide. Compared to the previous year, the 2026 exercises demonstrated a clearer effort to integrate civilian society with military preparedness structures, reflecting a growing recognition among Taiwanese authorities that parallel but separate civilian and military operations would likely prove insufficient under actual conflict conditions. Such cooperation makes it possible to identify vulnerabilities and emerging needs more quickly, while ensuring that community initiatives and volunteer efforts complement rather than duplicate official response mechanisms. In this way, civilian engagement can be directed toward areas where it provides the greatest added value, particularly in situations where military or governmental capacities may be temporarily constrained.

The Lai administration has articulated an ambitious objective of preparing 400,000 citizens to actively participate in Taiwan's broader societal resilience framework. By March 2026, more than 100,000 individuals had already completed various forms of civil defense and emergency preparedness training. At the same time, the development of societal resilience in Taiwan has not been driven exclusively by state institutions. A wide range of nongovernmental actors, including civic organizations, community initiatives, and religious groups, have become increasingly involved through training programs, educational activities, and disaster-relief support for local communities.

Although both governmental and nongovernmental efforts constitute essential pillars of Taiwan's resilience strategy, an important structural tension remains. On the one hand, political leaders, including President Lai himself, have repeatedly emphasized that civil society organizations should play a supportive and complementary role alongside state institutions in strengthening national preparedness. On the other hand, the operational structures of these organizations remain largely outside formal governmental coordination mechanisms, as they are neither institutionally nor legally integrated into Taiwan's civil defense and emergency response architecture.

A Top-Down Agenda Instead of Structural Support

There is little doubt that the government's strategy of building a resilient society, including consultations with civil society representatives, is an important step toward improving coordination during crises. At the same time, however, persistent structural shortcomings in cooperation between governmental and civic actors, as well as the persisting tendency to treat nongovernmental organizations as secondary to the state, have limited the effectiveness of these efforts. Consequently, many civil society organizations directly engaged in resilience-building and emergency preparedness have increasingly voiced concerns regarding the insufficiency of existing governmental measures following the announcement of President Lai's strategy.

One of the central criticisms concerns the still limited integration of civil society organizations and private-sector actors into Taiwan's broader resilience architecture. Taiwanese NGOs frequently constitute the first line of response during crises. Moreover, they

are increasingly recognized as important watchdogs in the context of escalating cross-Strait tensions, particularly through fact-checking and public education efforts aimed at countering disinformation originating from China.¹¹ Nevertheless, mechanisms for coordination, communication, and operational integration between the government and civic actors remain underdeveloped. As a result, observers and advocacy groups have called for the establishment of clear channels for verification, coordination, and communication during emergencies.¹²

Currently, dozens of Taiwanese civil society organizations provide training and workshops on civil defense and emergency preparedness. Yet their research, materials, and policy recommendations are rarely incorporated into governmental initiatives, often resulting in the duplication of existing efforts. One example is the government's civil defense guide, which did not substantially draw from the handbook produced by Watchout, a prominent Taiwanese civic media organization and NGO that focuses on government transparency, political accountability, and civilian defense preparedness.¹³ Many observers argued that government-issued guide lacked practical relevance and failed to address the realities faced by ordinary civilians. This criticism came not only from NGO representatives and subject-matter experts, but also from some members of the ruling Democratic Progressive Party (DPP).¹⁴ This episode reinforced concerns that Taiwan's resilience initiatives remain overly centralized and insufficiently connected to existing grassroots networks and expertise.

Another major challenge concerns scaling up and institutionalizing civil defense solutions developed by nongovernmental actors. Organizations like Kuma Academy and Forward Alliance have expanded civil defense training, preparedness handbooks, and educational activities across large parts of Taiwan. However, despite their effectiveness, they cannot

match the reach of the state. One example of a potentially national-scale solution is Forward Alliance's recently released iCanHelp app (see <https://www.forward.org.tw/en/a/resources/app>) designed to help civilians prepare for disasters and crises through interactive maps, real-time information sharing, photo uploads, and the identification of shelters and supply points. Integrating such tools with public emergency-response systems could significantly improve disaster management capabilities while also extending access to citizens who may never learn about NGO-developed applications independently.

The broader structure governing cooperation between state and civil society also raises concerns. Although the WOSDR Committee formally includes NGO and civil society representatives, it does not yet constitute a stable or institutionalized framework for long-term cooperation. To date, the committee has convened only seven times, limiting both continuity and the practical depth of engagement between governmental and nongovernmental actors. Moreover, civil society representatives participating in the committee must compete for limited discussion time and agenda-setting opportunities not only with government officials, but also with ministry representatives and technical experts from various sectors. This reduces their ability to contribute consistently to policymaking.

At the same time, the establishment of the committee directly under the Presidential Office is not without strategic justification. Taiwan's civil defense and resilience system has historically been fragmented across multiple ministries and local government structures, with responsibilities divided among institutions such as the National Security Council, the Ministry of the Interior, the Ministry of Health and Welfare, and the Ministry of National Defense. In this context, presidential coordination creates a mechanism capable of forcing inter-agency

cooperation, aligning initiatives across institutions, and elevating societal resilience into a broader national priority. The public nature of the committee's meetings additionally reflects its symbolic and strategic role in mobilizing society and signaling to international partners that Taiwan treats resilience and self-defense seriously.

Nevertheless, questions remain regarding the long-term durability and practical effectiveness of the current framework. Because the committee functions primarily as a presidential advisory body rather than as a permanent institution embedded within a ministry or formal administrative framework, it is unlikely to be the central mechanism through which regulations and operational policies are systematically implemented. Its continuity may therefore depend heavily on the priorities of a particular presidential administration. This creates uncertainty about whether the current model of state-civil society cooperation would survive a future change of government. Such concerns are reinforced by visible political tensions between opposition actors, particularly the Kuomintang and organizations associated with civil defense and resilience-building initiatives, including Kuma Academy.¹⁵

For this reason, establishing a permanent ministerial unit dedicated specifically to cooperation with civil society organizations could serve as an important complementary mechanism. Such a body could help ensure continuity beyond individual presidential administrations while also translating the committee's strategic discussions into day-to-day institutional coordination. It could prepare policy proposals in advance of committee meetings, facilitate interagency implementation, and maintain regular operational cooperation with NGOs and grassroots organizations on an ongoing basis. Without such an institutional anchor, the current arrangement provides only limited assurance that cooperation with civil

society organizations will remain politically supported and operationally sustained under a different administration.

Conclusion

Taiwan's evolving strategy of building "whole-of-society resilience" under the Lai administration represents a significant attempt to strengthen societal preparedness in response to growing security threats and potential crisis scenarios. The increasing integration of civilian preparedness exercises with military planning demonstrates a gradual shift toward a more comprehensive resilience model. At the same time, this analysis highlights substantial structural limitations in cooperation between the state and civil society. Although Taiwanese NGOs have developed advanced preparedness programs and community-based response mechanisms, their activities remain only partially integrated into formal governmental structures.

Top-down policymaking, insufficient local-level coordination, and the absence of permanent institutional frameworks for cooperation continue to hinder the more effective development of social resilience and strengthening of civil society. Consequently, enhancing long-term coordination between the state and society, improving local resilience networks, and institutionalizing cooperation with nongovernmental actors remain essential challenges for the future development of Taiwan's societal resilience strategy.

Policy Recommendations

- **Institutionalize Continuous State and Civil Society Cooperation:** Establish a permanent and structured mechanism for cooperation between governmental institutions and civil society organizations that operates on a continuous rather than ad hoc basis. Such a framework should provide NGOs and grassroots organizations with meaningful opportunities to present, test, and discuss resilience solutions that could later be integrated into national preparedness strategies and emergency-response systems.
- **Create a Dedicated Governmental Body for Civil Society Cooperation:** Develop a specialized governmental unit responsible for long-term coordination with civil society organizations within one of Taiwan's ministries or central administration institutions. Comparative examples from Europe demonstrate the advantages of institutionalized cooperation frameworks, such as Finland's Advisory Board on Civil Society Policy (KANE) operating under the Ministry of Justice, Poland's ministerial-led office responsible for civil society affairs, and specialized offices for NGO cooperation established in countries such as Croatia, Estonia, and Slovenia.
- **Establish Transparent Public Grant Mechanisms for Civil Society Resilience Projects:** Expand opportunities for NGOs and community organizations to implement publicly funded resilience and preparedness projects with the possibility of later integration into governmental emergency response frameworks. To ensure transparency and reduce political influence over funding decisions, Taiwan should establish a centralized governmental institution or coordinating body responsible for administering open and competitive grant programs, rather than relying primarily on discretionary commissioning by individual ministries.
- **Strengthen Cooperation Between Local Governments Structures and Grassroots Organizations:** Introduce a state-supported program aimed at integrating local government institutions with grassroots organizations, local NGOs, and community groups to develop shared crisis-management and disaster-response structures at the municipal level. Such initiatives should prioritize locally oriented preparedness mechanisms capable of responding rapidly to natural disasters, infrastructure disruptions, or security crises, thereby reducing excessive dependence on central government intervention during emergencies.

Endnotes

¹ NATO, "Resilience, civil preparedness and Article 3", November 13, 2024. <https://www.nato.int/en/what-we-do/deterrence-and-defence/resilience-civil-preparedness-and-article-3>

² Olga Kutsenko, "Resilience under fire: navigating societal challenges, agency, and innovation in times of war", *Innovation: The European Journal of Social Science Research*, 38(1), 1–10, 2025. <https://doi.org/10.1080/13511610.2025.2465177>

³ Wen-Chen Chang and Chun-Yuan Lin, "Taiwan: Democracy, Technology, and Civil Society", in Victor V. Ramraj, ed., "Covid-19 in Asia: Law and Policy Contexts" Oxford University Press, January 21, 2021, pp. 43–56. <https://doi.org/10.1093/oso/9780197553831.003.0003>

⁴ Valerii Pekar, "Civil Society in Ukraine: a Sled Dog, Not a Watchdog", in Piotr Kosiewski, ed., "Resilience and Solidarity: Ukrainian Civil Society in the Face of War", Stefan Batory Foundation, 2025, pp. 67–79. https://www.batory.org.pl/wp-content/uploads/2025/03/Resilience.and_.Solidarity_report_ENG.pdf

⁵ Ministry of National Defense of Taiwan, "All-Out Defense Contingency Handbook", 2023. https://adma.mnd.gov.tw/files/web/191/file_up/100004/1392/All-Out%20Defense%20Contingency%20Handbook.pdf

⁶ Lee Hsi-min and Eric Lee, "Taiwan's Overall Defense Concept, Explained", *The Diplomat*, November 3, 2020. <https://thediplomat.com/2020/11/taiwans-overall-defense-concept-explained/>

⁷ Office of the President of Taiwan, "Whole-of-Society Defense Resilience Committee: About the Committee", 2024. <https://english.president.gov.tw/Page/670>

⁸ All-out Defense Mobilization Agency, "The 2025 Urban Resilience (All-Out Defense Mobilization) Exercises of Kinmen County will be carried out on June 12, 2025", June 4, 2025. <https://adma.mnd.gov.tw/uniten/100005/7873>

⁹ Tom Wilson, "What Taiwan's Resilience Planning is Missing", *Taiwan Insight*, May 26, 2026. <https://taiwaninsight.org/2026/05/26/what-taiwans-resilience-planning-is-missing/>

¹⁰ All-out Defense Mobilization Agency, "2026 Urban Resilience (All-Out Defense Mobilization) Exercises", April 8, 2026. <https://adma.mnd.gov.tw/uniten/100003/7764>

¹¹ CIVICUS, "TAIWAN: 'Civil society plays key roles in tackling natural disasters and man-made threats, notably from China'" [Interview with Hsin-Huang Michael Hsiao], April 24, 2024. <https://civicus.org/index.php/media-resources/news/interviews/6985-taiwan-civil-society-plays-key-roles-in-tackling-natural-disasters-and-man-made-threats-notably-from-china>

¹² Article 19, "Taiwan: Building whole-of-society resilience in face of crisis", April 9, 2025. <https://www.article19.org/resources/taiwan-building-whole-of-society-resilience-in-face-of-crisis/>

¹³ Formosa News, "Watchout to publish second edition of its civil defense handbook", July 12, 2023. <https://english.ftvnews.com.tw/news/2023712W09EA>

¹⁴ Jake Chung, "Group to publish more accessible civil defense guide", *Taipei Times*, July 13, 2023. <https://www.taipeitimes.com/News/front/archives/2023/07/13/2003803107>

¹⁵ Lin Hsin-han, Huang Ching-hsuan, Esme Yeh, "KMT lawmakers question Kuma Academy fundraising", *Taipei Times*, January 7, 2025. <https://www.taipeitimes.com/News/taiwan/archives/2025/01/07/2003829791>

Beyond the Seven Sons

Taiwan and Europe's Shared Research Security Challenge

By Daria Impiombato

Amid Beijing's pressure to unify Taiwan with the People's Republic of China (PRC), Taipei cannot afford to lose its political and technological edge if it is to maintain the island's self-governing status. That edge rests on technological leadership as well as democratic legitimacy, placing Taiwan at the heart of great-power competition. It is essential for Taiwan and democratic nations actively trying to preserve democratic institutions to work together to counter authoritarian influence, especially in core strategic sectors such as academia.

Academia sits where technological leadership and democratic legitimacy meet. The Chinese Communist Party (CCP) persistently seeks to penetrate multiple layers of Taiwan's academic and cultural ecosystems to cultivate dependencies and, ultimately, shape consensus on the island in support of Beijing's unification agenda. This makes academia a critical arena in which competition between the PRC and Taiwan—and by extension between the PRC and the United States—unfolds. While the PRC's targeting of Taiwan is uniquely intense given the island's centrality to Beijing's strategic objectives,¹ concerns around research integrity and academic freedom in the context of authoritarian influence are increasingly shared across liberal democracies.

In several EU member states as well as in EU institutions, these concerns come together under the frameworks of "research security", "knowledge security", and "trusted research". Over the past decade, policymakers have increasingly recognized

the need for systems that preserve openness and dynamism in academic and research environments while safeguarding academic integrity, democratic values, and national security interests.

This is a difficult balance to strike, especially for Taiwan, which reveals how universities are exposed not only to the PRC's military-civil fusion and technology transfer risks, but also to political influence and co-optation. Governments have developed a range of ad hoc responses and institutional frameworks to define and manage these challenges, but the development of effective capacity in institutional and geographical silos is neither efficient nor sufficient.

Last year, Taiwan's President Lai Ching-te addressed European lawmakers, emphasizing the importance of Taiwan-Europe collaboration in safeguarding democratic institutions from authoritarian infiltration.² Cooperation would enable both sides to treat research security as a comprehensive challenge encompassing military and dual-use technologies as well as political influence and coercion while preserving academic freedom and the openness that underpins the value of democratic research systems. Within this framework, academia and related research bodies should play a central role.

Beijing's Competitive and Political Interests Target Academia

PRC institutions that establish ordinary academic collaboration with institutions elsewhere can facilitate productive scholarship on both sides, but this collaboration can also be a vector for technology transfer and political influence with adverse consequences for those other institutions and nations. In parallel to its activities vis-à-vis Taiwan, the CCP has been developing levers to shape knowledge production and public discourse around its political red lines in countries around the world.

One of the CCP's core objectives is to win the technological competition with the United States and achieve greater technological self-sufficiency while also building a techno-powered world-class military. Its military-civil fusion strategy is central to this effort, actively promoting the integration of civilian research and military modernization.³ A second, less visible but equally important objective is to preserve the CCP's grip on power by shaping the domestic and international environments in ways that align with its core interests.

PRC universities therefore operate simultaneously as channels for technological acquisition and as instruments of political influence. China uses academic cooperation not only to support military modernization and technological self-sufficiency within its borders, but also to shape knowledge production and normalize its preferred political order elsewhere—nowhere more clearly than in Taiwan. Military-civil fusion and political influence strategies converge in their effect: Both seek to constrain Taiwan's autonomy by absorbing critical technologies and talent while gradually drawing society into Beijing's orbit.

Pursuing Technological and Military Supremacy

Rather than separate civilian and defense research, the PRC actively seeks to integrate the two within a unified strategic ecosystem. This is particularly evident in dual-use fields such as semiconductors, artificial intelligence, aerospace, quantum technologies, biotechnology, and advanced materials. A recent study based on nearly 3,000 People's Liberation Army (PLA) AI-related contract awards from 2023 and 2024 shows, for example, that military procurement increasingly relies on civilian universities and commercial firms. It concludes that the PLA's technological modernization is no longer confined to traditional defense institutions but is embedded across China's broader innovation system.⁴

As a result, the research security challenge extends well beyond the PLA academic and research institutions, the so-called Seven Sons of National Defense—the military-linked universities that Taiwan formally sanctioned last year.⁵ Given the integrated nature of contemporary scientific research, simple blacklist-based approaches have become insufficient. For instance, the Australian Strategic Policy Institute's China Defense Universities Tracker identifies numerous ostensibly civilian universities that host defense laboratories, hold sensitive security credentials, or maintain other links to defense, intelligence, and critical technology research.⁶

Taiwanese analyses have repeatedly warned that academic cooperation can directly contribute to the PLA's modernization efforts, particularly through defense-linked institutions and dual-use research fields.⁷ However, for Taiwan, protecting critical technologies requires moving beyond institutional labels toward a more granular understanding of risk, incorporating research outputs, talent flows, collaborative projects and exchanges, as well as other

linkages that may ultimately feed into the PRC's military modernization.

Aligning Academia with Beijing's Interests

For the CCP, influencing and co-opting strategic members or groups of society outside the party is part of a broad and increasingly institutionalized political strategy known as the "united front".⁸ Academic and research communities have long been a target of united-front activities and should therefore be understood as operating within a broader CCP influence ecosystem, not merely as potential conduits for technological transfer or military modernization efforts.

The CCP is particularly focused on questions of sovereignty and regime legitimacy. In the case of Taiwan, it uses education and culture as instruments to deepen cross-Strait integration and advance support for unification. Official PRC discourse explicitly frames educational and cultural exchanges as components of a broader integration strategy. For example, the Taiwan Affairs Office's promotion of the Fujian cross-Strait integration zone frequently emphasizes creating conditions that encourage people in Taiwan to be "willing to come, stay, integrate and develop well" on the mainland.⁹

Recent remarks by Politburo member Wang Huning during a visit to the PRC by the chairwoman of Taiwan's main opposition party, the Kuomintang, linked cultural and educational work to strengthening a shared Chinese cultural identity, opposing "Taiwan independence" and "de-Sinicization", and guiding youth toward the "correct" view of history, nationality, and country. In this framing, academic and youth exchanges are intended to cultivate attachment

to China and normalize Beijing's preferred vision of cross-Strait unification.¹⁰

United front work therefore operates through universities, youth exchanges, internships, research platforms, and even primary and secondary schools to cultivate these ties. A recent example is the creation of a "Community for Cross-Strait Integrated Development of Academic Research" by Huaqiao University, Huai'an University and Zhaoqing University.¹¹ The initiative is framed around deepening integrated development to promote "spiritual harmony" across the Strait and advance peaceful reunification.

Huaqiao University is also one of the three universities sanctioned by Taiwan in 2025 because of their links to the CCP's United Front Work Department.¹² The ban, which is distinct from the "Seven Sons" severance, expanded the definition of research security beyond institutions directly tied to the military to include universities whose primary strategic value lies in united front work. Such measures, however, still do not effectively address a much broader ecosystem of influence that extends well beyond formal institutional affiliations.

On the one hand, academic and research cooperation with the PRC can open the way to technology leakage and talent recruitment in strategically important sectors.¹³ On the other hand, university-led cultural exchanges and academic platforms can further political co-optation and influence goals by shaping students' and scholars' exposure to, and acceptance of, Beijing's preferred narratives.¹⁴

While Taiwan is the most exposed case, there is now substantial evidence that "China's influence activities can result in censorship, intimidation, and harassment that shape critical discourse about China in universities around the world."¹⁵ One recent

example is reported pressure directed at Sheffield Hallam University in the UK over its research program on forced labor.¹⁶ Yet outside Taiwan, many still treat these incidents as isolated controversies rather than as part of a broader, systemic research-security challenge.

International Response Needs a Coordinated, Comprehensive Approach

Academia has become a contested space and, beyond concerns over technology transfer and institutional influence, researchers themselves increasingly face coercion and surveillance risks. However, countries have so far adopted different approaches to addressing these challenges, complicating coordination efforts, particularly given the transnational nature of the issue.

Taiwan has restricted exchanges with the Seven Sons of National Defense to mitigate military and dual-use technology risks, while acting against universities linked to the United Front Work Department to address political influence, and using degree-recognition and exchange controls to limit institutional exposure and prevent dependencies. These measures are steps in the right direction, but blacklist-based approaches fall short of an effective response to the integrated nature of the challenge and remain largely reactive and institution-specific. More comprehensive and sustained scrutiny is needed to capture the full scope of the threat.

European debates are also moving beyond a narrow focus on military-relevant research and dual-use technologies. In its 2025 position paper, for example, Germany's Council of Science and Humanities argued for the concept of "knowledge security", which covers

not only research activities but also staff and student exchanges while aiming to protect both national interests and academic freedom. It also adopted the EU's broader research-security framing, which includes undesirable knowledge transfer, malign influence, self-censorship, and violations of academic freedom and research integrity.¹⁷ The implementation, however, is still in the making and has so far, similar to Taiwan, resulted in ad hoc bans at times initiated by single universities.¹⁸

At the EU level, the 2024 Council Recommendation (reacting to European Commission proposals) on enhancing research security defines the issue as entailing three risks: the undesirable transfer of critical knowledge and technology, malign influence on research—such as disinformation, self-censorship, and pressure on researchers—and ethical or integrity violations where knowledge is used to undermine fundamental rights and democratic values. The European Commission particularly highlights high-risk sectors such as advanced semiconductors, AI, quantum technologies, and biotechnology, but the framework is intentionally broader than dual-use technology alone. It recognizes that universities can be vulnerable not only through laboratories and patents, but also through student exchanges, institutional partnerships, and political influence operations.¹⁹

Toward a New Ecosystem of Safe Academic Research

Academic communities in both Taiwan and Europe place freedom and openness at the center of their efforts to pursue progress and innovation, but if exploitation from external actors is not prevented, freedom and openness risk being gradually eroded. While Taiwan is ahead in recognizing political influence

as a research security issue, Europe has been more concerned with building institutional frameworks.

Exchanges on academic integrity would aid both Taiwan and partners in Europe to streamline their efforts and better detect and respond to threats. Europe could benefit from Taiwan's experience and expertise in dealing with political influence, while Taiwan could broaden its approach by adopting Europe's comprehensive research security framework.

The following steps should be taken:

- Governments should support universities in developing clear guidance for participation in exchanges and talent programs identified as higher risk and restrict those that do not meet pre-established security criteria. To address political influence more directly, governments should also invest in training and awareness-raising across relevant administrative levels in both government and academia, with a particular focus on the CCP's united front activities.²⁰
- Frameworks developed through international cooperation should incorporate common, sector-wide due diligence standards. High-risk university screening should be expanded to include nonofficial party and military-linked organizations, and each collaboration should undergo a rigorous risk assessment.
- Efforts in both Taiwan and Europe should focus on building shared knowledge bases capable of vetting institutions, funding sources, and sensitive technology areas quickly and avoiding a heavy bureaucratic burden. Monitoring and evaluation should continue throughout the course of cooperation to track access to sensitive

research, data-sharing practices, and personnel mobility.

- Additional mechanisms should be developed to track research output and intellectual property, particularly in dual-use technology areas, to better access pathways of downstream transfer and potential end-use applications.

Such an approach would not only set clear boundaries to protect the academic freedom underpinning democratic systems; it would also help ensure that highly valuable but vulnerable academic and research communities can thrive, supported by appropriate resources and security safeguards.

Endnotes

¹ Chris Buckley, "Xi Is Poised to Press Trump on Arms Sales to Taiwan", *The New York Times*, May 15, 2026. <https://www.nytimes.com/2026/05/12/world/asia/xi-trump-china-taiwan-arms-sales.html>

² Reuters, "Taiwan, EU both face threats of external infiltration, president tells European lawmakers", July 22, 2025. <https://www.reuters.com/world/china/taiwan-eu-both-face-threats-external-infiltration-president-tells-european-2025-07-22/>

³ Richard A. Bitzinger, Yoram Evron, and Zi Yang, "China's Military-Civil Fusion Strategy: Development, Procurement, and Secrecy", *Asia Policy*, 16 (1), January 2021. https://www.nbr.org/wp-content/uploads/pdfs/publications/ap16-1_china_mcf_rt_jan2021.pdf

⁴ Cole McFaul, Sam Bresnick, and Daniel Chou, "Pulling Back the Curtain on China's Military-Civil Fusion", *Center for Security and Emerging Technology*, September 2025. <https://cset.georgetown.edu/publication/pulling-back-the-curtain-on-chinas-military-civil-fusion/>

⁵ Rachel Lin and Jonathan Chin, "Seven Chinese universities sanctioned", *Taipei Times*, March 1, 2025. <https://www.taipeitimes.com/News/front/archives/2025/03/01/2003832691>

⁶ Australian Strategic Policy Institute, "Home", *China Defence University Tracker*, 2026. <https://unitracker.aspi.org.au/>

⁷ 陳穎萱 (Chen Yingsuan), "中共利用學術合作促進軍事現代化" [The CCP promotes military modernization through academic cooperation], *Institute for National Defense and Security Research*, December 24, 2021. <https://indsr.org.tw/respublicationcon?pid=1246&resid=840&typeid=3&uid=12&utm>; 董慧明 (Tung Hui-Ming), "大陸「軍民融合」發展戰略之現況與問題評析" [An Analysis of Current Situation and Problems of PRC "Civil-Military Integration Development Strategy"], *Taiwan Ministry of Justice Investigation Bureau*, March 2016. https://www.mjib.gov.tw/FileUploads/eBooks/q41e22203fd64826a2ae2a100baa4bce/Section_file/1fc0998fdcb74409b354aa80c0ee2b31.pdf

⁸ Cheryl Yu, "Beijing's United Front and the Quiet Transfer of Western Technology", *War on the Rocks*, April 27, 2026. <https://warontherocks.com/beijings-united-front-and-the-quiet-transfer-of-western-technology/>

⁹ Taiwan Work Office of the CPC Central Committee, "国新办举行《中共中央 国务院关于支持福建探索海峡两岸融合发展新路建设两岸融合发展示范区的意见》发布会" [The State Council Information Office held a press conference on the "Opinions of the CPC Central Committee and the State Council on Supporting Fujian in Exploring New Paths for Cross-Strait Integrated Development and Building a Cross-Strait Integrated Development Demonstration Zone."], September 14, 2023. <https://archive.is/5glyv>

¹⁰ Xinhua News Agency, "王沪宁会见出席第三届海峡两岸中华文化峰会两岸文化界人士代表" [Wang Huning met with representatives from the cultural circles from both sides attending the 3rd Cross-Strait Chinese Culture Summit], May 11, 2026. <https://www.xinhuanet.com/20260511/04a4268c58894c02a446f85b4ff7aca9/c.html>

¹¹ Zhaoqing University, "我校与苏闽两校携手共建两岸融合研究新平台" [Zhaoqing, Jiangsu and Fujian universities are joining hands to build a new platform for cross-strait integrated research], March 23, 2026. <https://archive.is/gQkOF>

¹² Lawrence Chung, "Taiwan bans academic exchanges with 3 mainland Chinese universities", *South China Morning Post*, February 20, 2025. <https://www.scmp.com/news/china/politics/article/3299492/taiwan-bans-academic-exchanges-3-mainland-chinese-universities>

¹³ The Control Yuan, "多名臺灣科學者遭中國挖角 有無違反兩岸人民關係條例 監察委員賴振昌、葉大華、蕭自佑及蘇麗瓊申請自動調查" [Several Taiwanese researchers have been poached by China. Has this violated the Act Governing Relations between the People of the Taiwan Area and the Taiwan Strait? Control Yuan members Lai Zhenchang, Yeh Ta-hua, Hsiao Tzu-yu, and Su Li-qiong have applied for an investigation], February 26, 2021. https://www.cy.gov.tw/News_Content.aspx?n=528&s=20065; 陳穎萱 (Chen Yingsuan), "中共利用學術合作促進軍事現代化" [The CCP promotes military modernization through academic cooperation], *Institute for National Defense and Security Research*, December 24, 2021. <https://indsr.org.tw/respublicationcon?pid=1246&resid=840&typeid=3&uid=12&utm>

¹⁴ Chris Horton, "Taiwanese universities may be self-censoring political discussion to attract Chinese students", *Quartz*, July 20, 2022. <https://qz.com/925184/taiwanese-universities-may-be-self-censoring-political-discussion-to-attract-chinese-students>

¹⁵ U.S.-China Economic and Security Review Committee, "2023 Annual Report, Chapter 2, Section 2: Battling for Overseas Hearts and Minds: China's United Front and Propaganda Work", November 2023, p. 224. https://www.uscc.gov/sites/default/files/2023-11/Chapter_2_Section_2--Chinas_United_Front_and_Propaganda_Work.pdf

¹⁶ Damian Grammaticas, "China intimidated UK university to ditch human rights research, documents show", *BBC*, November 3, 2025. <https://www.bbc.com/news/articles/cq50j5vwny6o>

¹⁷ German Science and Humanities Council, "Science and security in times of global political upheaval" [Position paper], May 2025. https://www.wissenschaftsrat.de/download/2025/2485-25_en.pdf

¹⁸ German Science and Humanities Council, "Science and security".

¹⁹ European Council, "Council recommendation of 23 May 2024 on enhancing research security", *Official Journal of the European Union*, May 30, 2024. <https://eur-lex.europa.eu/eli/C/2024/3510/oj/eng>

²⁰ Yu, "Beijing's United Front".

Civic Culture at the Heart of Taiwan's Digital Democracy Paradox

By Lauren Kirby

Few questions are more pressing in 2026 than how democratic countries will govern AI use and increasingly omnipresent surveillance technology. Taiwan finds itself at the heart of both issues, as home to the majority of AI chip production globally and a developing democracy with a recent history of innovative digital participatory governance practices. Taiwan's online civic culture is even more relevant and urgent following the January 2026 AI Basic Act, which codifies democratic principles without creating a corresponding enforcement architecture.¹ Taiwan is one of the few places where the tension between enabling technology use and pursuing democratic goals is not only visible, but actively contested through civic participation and public deliberation, and it is therefore worth paying attention to.

The Rise of Civic Tech Participation

While it would be simple to ascribe the centrality of Taiwan in digital democracy policy debates to its role in the global AI supply chain, the reality is much more complex rooted in a rich culture of civic participation, rising from democratic struggles of the White Terror period (1949–1992)² and its accelerated modernization, powered by digital and online platforms, following the Sunflower Movement in 2014.³ Distrust of government, concerns about transparency, and demand for countering power in the hands or keyboards of the people drove modern civic technology adaptations. Taiwan's history of

authoritarian rule cultivated a political culture in which citizens viewed participation, scrutiny, and transparency as democratic responsibilities. This created a fertile civic environment for popular decentralized civic tech movements and platforms, such as g0v (g0v.tw/intl/en/) and vTaiwan (www.vtaiwan.tw/) to harness citizen action and build transparent, state-adjacent digital infrastructure where the government proved unwilling to act.

These “do-it-yourself” models combined the willingness of Taiwanese citizens to engage in governance issues with digital deliberation innovations to build systems and processes that inform government decisions and hold state actors accountable. Since 2014, Taiwan's civic tech participation movement has achieved significant domestic legislative and policy influence. One result has been the creation of Public Digital Innovation Space (PDIS) in government to advance digital transformation and civic groups' engagement with AI governance that shaped the National Human Rights Commission's recommendations for the AI Basic Act. Civil-society recommendations will likely influence the ongoing two-year grace period that provides time for government agencies to align their regulations and administrative procedures with governance principles of the AI Basic Act.⁴ Furthermore, Taiwan's model has earned substantial international recognition, with leading AI and governance technical experts from Chatham House and practices.⁵

The Shadow of Surveillance Infrastructure

Taiwan's democratic civic technology ecosystem has developed in parallel to expanding state digital surveillance powers during and after the COVID-19 pandemic. Digital pandemic tools deployed included the 1922 contact tracing SMS system, digital health passes, and quarantine monitoring practices and tools such as digital fencing and the use of cell tower signals to enforce quarantine compliance. While Taiwan's health response was widely viewed as successful and used as an international standard, civil society and legal scholars have publicly debated and critiqued these efforts, and the civic tech community's own retrospective assessment of their contributions to Taiwan's digital governance draws a complicated picture. A 2024–2025 expert panel survey of g0v participants conducted by Dr. Shun-Ling Chen found that 43% of experienced civic tech respondents believed the government had failed to adequately inform the public about the privacy implications of the digital pandemic tools surveyed, including SMS check-in and mask map systems that originated in g0v community discussions before being deployed by the government⁶. The civic tech community's role in developing these participatory tools has not translated into community-wide endorsement of how the state deployed them, and this community increasingly exercises a watchdog role over their use.

These COVID-era practices established a pattern—deploy technology first and ask questions or institute safeguards later—while also creating institutional momentum that is now seen in other domains with uptake of rapid cross-agency data integration within and between public and private systems. Serving public health needs first, democratic deliberation of risks to privacy are often an afterthought that to date has been politically acceptable with no

major pushback from citizens or election-related consequences. While these decisions and actions had an enabling legal architecture that granted the executive branch a broad mandate to take “all necessary measures”,⁷ most surveillance tactics were put in place via the Central Epidemic Command Center's (CECC) daily press conferences, rather than through legislation or other public processes⁸. A 2024–2025 survey of legal professionals conducted by Hui-Chieh Su found that a majority of legal professionals surveyed judged these public communications measures alone to lack sufficient legal basis. One in four legal experts specifically opposed using press conference announcements to implement digital surveillance and rated digital fencing as the most severe privacy restriction of any tool deployed. Further, in the civic tech community survey, only 22% of respondents found it reasonable to use cell tower data for quarantine enforcement, which was among the government's first and most extensive deployments.⁹

More recently, Taiwan has again seen the Legislative Yuan (LY) take steps to act quickly in the interest of the public and to ask questions or initiate oversight and regulation later. In July 2024, the LY passed the Fraud Crime Hazard Prevention Act,¹⁰ which grants prosecutors and law enforcement access to communications user data and network traffic records with procedural standards that civil rights organizations have argued are weaker than those governing conventional wiretapping. Amendments in December 2025 expanded the scope of these powers and the Ministry of Interior used Article 42 of the Fraud Act to restrict, by administrative order, the popular social media platform RedNote without prior judicial review, citing information security issues and 756 fraud-related cases attributed to the platform.¹¹

Positive Developments and Challenges: Legislation and Enforcement

The National Health Insurance (NHI) database represents the most direct collision between surveillance-related and data collection approaches and the accountability architecture being built to contain them. The NHI database is Taiwan's largest, most detailed repository of personal health information. Civil society organizations sued over the unregulated secondary use of NHI data for AI research, and in 2022 the Constitutional Court ruled that Taiwan lacked a constitutionally adequate, independent, data protection mechanism and mandated that one be created within three years.¹² The ruling also mandated the establishment of an opt-out mechanism to allow individuals to prevent their data from being used for purposes outside the original scope and imposed fines up to NT\$10 million for unauthorized access.¹³ The NHI Data Management Act that the LY passed in December 2025 can be viewed as a judicially compelled correction. A related development illuminates how democratic pressure can, over time, constrain algorithmic power even without formal privacy law mechanisms. In early January 2026, the LY passed the Delivery Worker Rights Protection and Platform Management Act after four years of sustained worker organizing and persistent legislative engagement. Workers challenged delivery platform-controlled dispatch and compensation calculations run through opaque digital systems that offered them neither visibility nor recourse. Their efforts secured protections that increased worker safeguards, creating transparency and accountability in the digital economic systems.

Tensions between technological innovation and privacy have only intensified since the promulgation of the AI Basic Act against the backdrop of more than a decade of fragmented data protection

enforcement. Taiwan's Personal Data Protection Act¹⁴ set out data governance principles, but for years lacked the enforcement architecture needed to put them into practice. Although some enforcement measures existed, these processes, tools, and standards were dispersed across ministries taking sector-specific approaches, such as the Financial Supervisory Commission for finance and the Ministry of Health and Welfare for healthcare. The result was uneven interpretation and oversight, without the independence, cross-sectoral authority, or policy agility needed to appropriately manage risk in a platform-centric, AI-enabled world. First enacted in 1995 with modifications enacted in 2010 and in effect from 2012, the PDPA could not have anticipated the speed of AI adoption that would follow.

The November 2025 PDPA amendments represent significant structural reform since the Act's enactment: They vest centralized enforcement authority in the new Personal Data Protection Commission (PDPC), mandate data breach notification to affected individuals and the PDPC, introduce administrative inspection powers, and require government agencies to designate Data Protection Officers.¹⁵ Yet the shift from legislative text to operational governance remains incomplete. The PDPC cannot formally commence operations until the full chamber of the LY passes the PDPC Organization Act, which initiates the process for the Executive Yuan (EY) to set an effective date for the amendments and will actualize the creation of an independent, centralized supervisory authority.¹⁶ Civic actors, legal experts, and academics have been actively engaged in shaping how these laws will ultimately function, and the Act has cleared the Judiciary and Organic Laws Committee but not yet the full chamber. Only after these additional procedural steps are complete can the new personal data protection enforcement regime begin. In the interim, the Preparatory Office publishes draft subsidiary regulations for public

comment, such as inspection procedures and security maintenance standards, but none carries legal force and accountability gaps remain until the current status quo changes.

In this context, the AI Basic Act's shortest provision, Article 11, may prove to be the most consequential. Article 11 establishes a statutory hierarchy of innovation: Where the interpretation and application of other laws would obstruct the development of new technologies and their applications, innovation—subject to the Act's seven basic principles—takes priority.¹⁷ Article 11 is a key component of Taiwan's broader privacy policy landscape because it means the PDPA, which limits data collection or unauthorized data use, could in principle be subordinated to AI development goals in cases subject to interpretation. Civil society flagged these issues during the act's drafting, in so doing further normalizing a level of civic participation within highly technical governance debates that many countries prevent or avoid. The Taiwan Association for Human Rights (TAHR) and the Judicial Reform Foundation (JRF) raised the concern that the provision could function as a backdoor around existing privacy protections. The government's response argued that the act's seven principles constrain Article 11's application; this, however, depends on those principles being operationalized through enforceable implementing rules that have yet to be defined and will likely rely on the existence, authority, and enforcement tools of the independent PDPC. Taiwan's choice of a "principles-based" approach, aligned more closely with the United States and Japan than with the EU's compliance-based AI Act, reflects a deliberate judgment about regulatory friction that will ultimately prove either judicious or harmful over the long term.

The two-year implementation window of the AI Basic Act is a critical democratic accountability period in which specific regulators across finance, health,

employment, and other domains must review, amend, or issue new rules consistent with the Basic Act. Taken more broadly, this period will test whether Taiwan's democratic culture can meaningfully shape the operational rules governing AI and data use. The Ministry of Digital Affairs (MODA) must produce an AI risk classification framework, which was publicly targeted for the first quarter of 2026 but has not yet been released. This process could validate the concerns of legal professionals: A majority of legal professionals surveyed by Dr. Chen held that restrictions on personal freedom and privacy should be decided by the legislature rather than delegated to executive agencies¹⁸. However, taking an optimistic view, the processes over the next two years are potential avenues for civil society engagement and means to give agency to additional voices championing privacy protection and oversight.

The draft Data Innovation and Utilization Promotion Act, currently in LY deliberation, will be another stress test. Designed to create frameworks for sharing government and personal data as fuel for AI development, it sits in direct tension with the PDPA's data minimization requirements and the December 2025 NHI Data Management Act's restrictions on secondary health data use. The final version of the act will give an indication of whether an innovation-first hierarchy is being operationalized over privacy protections.

Conclusion

Taiwan's democratic evolution and its increasing use of digital surveillance to address real and perceived challenges is not a contradiction that can or should be easily resolved. Instead, Taiwan's situation shows us that the tension between innovation and rights is one that all democracies must embrace through

strong institutions, legal checks and balances, civic participation (digital and otherwise), litigation, and public debate. These components are necessary to the survival and vitality of democratic systems, not threats to be contained.

Over the past six months, Taiwan has experienced its most intensive period of digital governance legislation to date. While this does not reflect a fully coherent and coordinated policy design, it does stem from accumulated democratic pressures exerted by a range of actors. These legislative developments signal democratic progress and evolution that are necessary for the holistic health of the political system in the face of complex challenges accelerated and amplified by digital tools.

Taiwan's future will be shaped by how these components can function and the degree to which civil society can exercise agency through procedural participation mechanisms—such as PDPC comment periods and deliberations on the Data Innovation Act—and translate those opportunities into substantive regulatory safeguards and accountability provisions. Decisions about whether to pass the PDPC Organization Act to create meaningful, genuine enforcement capacity, how the draft Data Innovation and Utilization Promotion Act is shaped by civil society input to incorporate privacy protections, and the extent to which MODA's AI risk classification framework takes the PDPA's data minimization principles seriously will help define Taiwan's evolving democratic habits. They will also determine whether the AI Basic Act will support democratically oriented digital infrastructure or remain simply a technology promotion law with only nominal democratic safeguards.

Similar to efforts to replicate AI chip production overseas, Taiwan's recent policy and regulatory developments governing technology use are likely to

attract comparative analysis for potential application in other contexts. However, it is important to emphasize that Taiwan's most valuable democratic export is not any singular piece of legislation or innovative participatory platform. Rather, the key lesson lies in Taiwan's political culture, a culture built through decades of democratic struggle that embraces civic scrutiny of state digital power as normal, expected, and consequential—as, indeed, its greatest asset.

Endnotes

¹ National Science and Technology Council, ROC (Taiwan), "Artificial Intelligence Basic Act", January 14, 2026. <https://law.nstc.gov.tw/EngLawContent.aspx?id=10099&lan=E>

² Stephen J. Hartnett, Patrick Saho-Whea Dodge, "On Postcolonial Remembering and Democratic Openings in Taiwan: An Interview with Former Political Prisoner, Fred Chin", Public Seminar, September 26, 2019. <https://publicseminar.org/essays/on-postcolonial-remembering-and-democratic-openings-in-taiwan/>

³ Ming-sho Ho, "The Activist Legacy of Taiwan's Sunflower Movement", Carnegie Endowment for International Peace, August 2, 2018. <https://carnegieendowment.org/research/2018/08/the-activist-legacy-of-taiwans-sunflower-movement>

⁴ National Human Rights Council, ROC (Taiwan), "Recommendations of the National Human Rights Commission on the Draft Artificial Intelligence Fundamental Act", July 15, 2024. <https://nhrc-ws.cy.gov.tw/Downloaddashx?u=LzAwMS9VcGxvYWQvNDM3L3JlbGZpbGUpMTIzNzUvNzQzNy8xNjJkNjMyMiliNDg4LTRmM2UtYmM1Yy1kMDExNDYxYWYyYjMucGRm&n=UmVjb21tZW5kYXRpb25zIG9mIHRob2ZSB0YXRpb25hbCBldW1hbiBSaWdodHMgQ29tbWlzc2lvbiBvbiB0aGUgRHJhZnQgQXJ0aWZpY2IhbiBjbnRlbGxpZ2VvY2UgRnVuZGFtZW50YWwgQWN0LnBkZg%3D%3D>

⁵ Carl Miller, "Recursive Public: Piloting Connected Democratic Engagement with AI Governance", vTaiwan and Chatham House, 2025. https://www.academia.edu/108565406/Recursive_Public_Piloting_Connected_Democratic_Engagement_with_AI_Governance

⁶ Shun-Ling Chen, "WP4 (Taiwan) Civil Society Engagement Report, Expert Panel Survey on Civil Tech", HRJust, January 23, 2026. <https://hrjust.org/2026/01/23/civil-society-engagement-report-expert-panel-survey-on-civic-tech/>

⁷ C-F Lin, "Taiwan: Legal Response to Covid-19", in *The Oxford Compendium of National Legal Responses to Covid-19*, ed. Jeff King et al., Oxford University Press, 2021. <https://oxcon.ouplaw.com/display/10.1093/law-occ19/law-occ19-e18>

⁸ Ministry of Health and Welfare, ROC (Taiwan), "Safeguarding the community line of defense to create a positive new lifestyle for disease prevention", May 10, 2023. <https://covid19.mohw.gov.tw/en/cp-4786-53904-206.html>

⁹ Hui-Chieh Su, "WP4 (Taiwan) Civil Society Engagement Report, Expert Panel Survey on Legal Experts", HRJust, January 23, 2026. <https://hrjust.org/2026/01/23/civil-society-engagement-report-expert-panel-survey-on-legal-experts/>

¹⁰ Ministry of the Interior, "Fraud Crime Hazard Prevention Act", as amended January 1, 2026. <https://law.moj.gov.tw/ENG/LawClass/LawAll.aspx?pcode=D0080226>

¹¹ Keoni Everington, "Taiwan bans RedNote for one year over fraud cases", Taiwan News, December 5, 2025. <https://www.taiwannews.com.tw/news/6258944>

¹² Constitutional Court of ROC (Taiwan), "Summary of TCC Judgment 111-Hsien-Pan-13 (2022)" [Case on the National Health Insurance Research Database], August 12, 2022. <https://cons.judicial.gov.tw/en/docdata.aspx?fid=5535&id=347736>

¹³ The Overseas Community Affairs Council, ROC (Taiwan), "Taiwan's Legislature passes law to regulate personal health data", December 6, 2025. <https://www.ocac.gov.tw/OCAC/Eng/Pages/Detail.aspx?nodeid=329&pid=81926712>

¹⁴ Preparatory Office of Personnel Data Protection Commission, "Personal Data Protection Act", as amended November 11, 2025. <https://law.moj.gov.tw/Eng/LawClass/LawAll.aspx?PCode=10050021>

¹⁵ International Trade Trust Compliance Network, "New Developments in Taiwan's Personal Data Protection Act", January 16, 2026. <https://ittcnet.org/insights/new-developments-in-taiwans-personal-data-protection-act/>

¹⁶ Hannah Kuo and Chuck Liu, "The Impact of the Personal Data Protection Act Amendments on the Private Sector (Taiwan)", Lee, Tsai, & Partners, November 2025. <https://www.leetsai.com/the-impact-of-the-personal-data-protection-act-amendments-on-the-private-sector-taiwan?>

¹⁷ National Science and Technology Council, "Artificial Intelligence Basic Act".

¹⁸ Hui-Chieh Su, "Expert Panel Survey on Legal Experts".

From Risk to Resilience

Taiwan's lessons for European economic security

By Filip Krenek

The outbreak of the US conflict with Iran has drawn much attention to the Strait of Hormuz, one of the world's key maritime bottlenecks, through which passes roughly 27% of global maritime trade in crude oil and petroleum and 20% of trade in liquefied natural gas (LNG).¹ Following Operation Epic Fury and Iran's subsequent attacks on tankers and laying of sea mines, traffic in the strait has been largely blocked. Brent crude has surged above \$100 a barrel; war-risk insurance premiums are four to five times higher than previously. The UN Development Programme estimates that the conflict could cause up to \$300 billion in economic losses to the Asia-Pacific region.² Europe has been particularly hard hit by the growing energy prices and rerouted shipping, creating pressure that is rippling through the wider economy, exposing Europe's persistent fossil fuel dependency, supply chain fragility, and limited preparedness for such shocks.

While parallels are never perfect, there is a maritime corridor whose disruption would arguably have broader and more immediate consequences for Europe: the Taiwan Strait. According to the Center for Strategic and International Studies, more than one-fifth of global maritime trade by value and close to half of the world's container fleet passes through this waterway each year.³ Unlike energy corridors such as the Strait of Hormuz, the Taiwan Strait carries cargo dominated by high-value intermediate goods and semiconductors embedded in automotive, machinery, defense, electronics, and clean tech supply chains. A naval blockade or a military conflict

in the area would not merely raise prices but could halt Europe's manufacturing. During the 2021 semiconductor shortage, EU car production fell by 7% on average, with Germany down 13%, Spain 9%, and Italy 8%, leaving EU output 4 million cars below pre-pandemic 2019 levels.⁴ A Taiwan Strait disruption could be of a different order of magnitude entirely.

The EU has built, however imperfectly, partial frameworks to manage energy supply disruptions, but the bloc has not applied the same level of scenario planning, contingency design, or strategic prioritization to a shock that could prove even more disruptive. Rhodium Group estimates that a Taiwan blockade would put more than \$2 trillion of global economic activity at risk,⁵ while Bloomberg Economics has put the first-year cost of a full-scale conflict at roughly 9.6% of global GDP.⁶ Given its industrial dependence on Taiwanese semiconductors, the EU would be among the most exposed. Yet Europe continues to view the Taiwan Strait primarily through the prism of US-China relations rather than a direct economic security threat. For years, this has been a structural blind spot. And while Europe increasingly recognizes the risks associated with Taiwan, it has devoted far less attention to the ways in which the island has adapted to decades of geopolitical pressure. This paper argues that Taiwan's experience offers valuable lessons for strengthening Europe's own economic security, industrial resilience, and approach to trusted interdependence.

Strategic Indispensability

Europe's exposure to the Taiwan Strait reflects how global production networks are structured. Taiwan accounts for roughly 60% of global semiconductor foundry output and around 90% of the most advanced chips, with production overwhelmingly concentrated in a single company, the Taiwan Semiconductor Manufacturing Company (TSMC). No comparable capacity exists elsewhere at scale, and, with the acceleration of AI-driven demand, supply at the technological frontier is likely to tighten further. Even TSMC's overseas investments are unlikely to close this gap. Despite pressure to ease the rules for certain overseas fabs, the National Science and Technology Council maintains a strict "N-2" rule,⁷ whereby chips produced in offshore fabs are kept two generations behind Taiwan's domestic production. Research and development also remain firmly anchored in Hsinchu and Tainan.

TSMC Arizona's fab, for example, produces advanced 4-nanometer chips used in flagship smartphones, data centers, and AI applications. However, volume production of next-generation 3-nanometer chips, which deliver higher performance and greater energy efficiency for the most demanding computing applications, is not scheduled to start until the second half of 2027. Similarly, the Kumamoto fab in Japan focuses on mature chips, with 3-nanometer capacity not expected until 2028.⁸ The ESMC joint venture in Dresden, Germany, is dedicated to mature chips for the European automotive sector and industrial machinery rather than the leading-edge chips used to power the world's most advanced AI systems. Meanwhile, TSMC's domestic 3-nanometer capacity is projected to reach 180,000 wafers per month by the end of 2026, a 40% increase year-on-year, dwarfing its aggregate overseas output. And the production rate of its cutting-edge 2-nanometer chips, launched in late 2025, is already set to reach 100,000 wafers

per month in 2026.⁹ This is well ahead of its only serious rivals in this domain, Samsung and Intel.

TSMC's leading-edge technology is kept domestic, solidifying the island's position as the world's leading hub for cutting-edge semiconductor manufacturing. And the production of frontier chips is becoming more concentrated. In an era of weaponized interdependence, this creates not only a competitive advantage for Taiwan but also a form of embedded deterrence. It raises the economic costs of unilateral action, including coercive measures aimed at altering the status quo in the Taiwan Strait. Such concentration does not remove risk; it redistributes it. Disruption would cascade across countries and sectors, with limited supply alternatives and high adjustment costs.

Other economies are using similar strategies. Japan, for example, controls roughly 90% of the global market for photoresists used in advanced lithography and dominates several segments of semiconductor manufacturing equipment, making itself indispensable in specific segments with global reach.¹⁰ South Korea occupies an equivalent position in memory chips, and the Netherlands, through ASML, in extreme ultraviolet (EUV) lithography systems. Together, these technological chokepoints form an interdependent ecosystem in which removing any one node would degrade the entire system.

The EU should take a page out of Taiwan's playbook and aim to reshape interdependence rather than attempt to eliminate it. This means identifying segments in which European firms occupy system-critical positions and directing policy support, procurement preferences, and outbound-investment screening to bolster them and prevent critical technology leakage. This may include individual companies, such as ASML in lithography, Infineon and STMicroelectronics in automotive-grade chips,

Airbus in commercial aviation, or clusters of European industrial automation and machine-tool firms.

The 2023 European Economic Security Strategy rests on three pillars: promote, protect, partner.¹¹ Analysts and commentators often say that it lacks an additional “P” for “prevent”. An active economic security strategy should not only reduce the costs of a potential economic conflict, but also decrease the likelihood of one occurring. Indispensability can be a strong and effective form of deterrence. Without such leverage, Europe’s economic security strategy will remain largely defensive and reactionary.

Building “Non-Red” Supply Chains

Taiwan also demonstrates that reducing exposure to supply chain vulnerabilities cannot rely on domestic production alone. It may be strategic to control specific parts of the supply chain, but the scale, cost, and complexity of existing production networks make full relocation neither feasible nor efficient. The more viable approach is to build alternative supply chains with trusted partners while preserving the benefits of global trade integration. This is what President Lai Ching-te laid out in February 2025 in his vision of “non-red supply chains” that span democratic societies (i.e., the ability to bypass China at all tiers of the supply chain).¹²

This approach requires moving beyond de-risking through diversification toward building trusted ecosystems. Production networks of semiconductors, electronics, and advanced manufacturing are deeply interconnected, spanning materials, components, design, and assembly. Replacing a single node is insufficient if upstream and downstream dependencies remain concentrated in a single country.

The drone manufacturing industry illustrates this challenge. Although drones are largely produced for commercial markets, they have become indispensable dual-use technologies with major military applications. Chinese manufacturer Da-Jiang Innovations (DJI) controls roughly 90% of the global commercial drone market, with prices 50%–75% below comparable US-made systems, creating a dependency that is difficult to overcome through market forces alone.¹³ At the same time, Taiwan demonstrates that trusted alternatives can be developed. Taiwanese companies have emerged as key alternative suppliers of Chinese-made drones. In 2025, Taiwan exported 123,000 drones to Europe (a 35-fold increase on 2024) and 85,000 more in the first two months of 2026, with almost all routed via Czechia or Poland to Ukraine.¹⁴ Taiwanese firms are also extending their production in Europe, announcing new investments, especially in Central and Eastern Europe.

But the drone case also illustrates how difficult reaching the “non-red” goal is. Taiwan’s aim of removing all Chinese inputs from its supply chains remains aspirational. A 2025 study by Taiwan’s Research Institute for Democracy, Society and Emerging Technology¹⁵ found that Taiwanese unmanned aerial vehicle producers still depend on imports from allied countries for specialized chips and software for flight control, positioning, and communication, and on Chinese raw materials such as rare-earth magnets and battery-cell inputs. The cost premium is significant: Taiwanese drones are priced roughly 25% more than Chinese equivalents—in some segments three to four times more—in part because Beijing has long subsidized its domestic industrial players in strategic sectors. Many Taiwanese drone companies are also family-run businesses that retain informal ties to mainland China, sometimes through relatives, complicating “non-red” certification required by official military contractors.¹⁶

Taiwan is nonetheless making progress. The Ministry of Economic Affairs (MOEA) launched the Taiwan Excellence Drone International Business Opportunities Alliance in 2024,¹⁷ bringing together over 200 manufacturers under a transparent-supply-chain standard. Taiwanese drone manufacturers are also increasing their efforts to sell to non-military government services, with one drone manufacturer receiving the Blue UAS certification for use by the US military. To ramp up domestic capacity and bring down production costs, the Taiwanese Defense Ministry announced an NT\$50 billion procurement in 2026–2027 (approx. \$1.6 billion).¹⁸ This defense contract, along with several others still in preparation, is part of the government's broader effort to reach an annual production of 180,000 drones, a goal that may be attained by 2028, two years earlier than initially targeted.¹⁹

Building “non-red” capacity takes years and sustained public money, but Taiwan's model that brings together an industry alliance, a certification scheme, anchor procurement, and partner countries provides a template that Europe can apply to its own dependencies, whether it be on Chinese batteries, solar wafers, rare-earth magnets, or electric-vehicle components. Europe should also aim to extend its industrial coordination beyond its borders, encouraging partners to specialize in complementary segments of strategic value chains rather than duplicate entire production systems. Such specialization transforms asymmetric dependence into trusted interdependence by distributing critical capabilities across a network of partners rather than concentrating them in a single high-risk supplier.

Three Lessons

The EU and Taiwan share similar understandings of economic security risks, but they differ in how they translate these into policy action. Taiwan's approach is shaped by constant pressure, where disruption is not treated as a low-probability event but as something that can occur at any time. This has led to a more practical way of working: close coordination between government and industry, monitoring of supply chain risks, and the ability to adjust relatively quickly when conditions change. Several examples illustrate this.

First, Taiwan has institutionalized civil-military and government-industry coordination through the Whole-of-Society Defense Resilience Committee established in 2024 and chaired by President Lai.²⁰ The committee works on five areas of resilience and crisis preparedness, including energy and critical infrastructure and strategic material and supply chain preparedness, and it prepares strategies for gray-zone, naval-blockade, and conflict scenarios. The use of tabletop exercises and drills is a well-established practice in Lai's government, as demonstrated by the 2025 Urban Resilience Exercise, which combined disaster response, military exercise, and air-raid drills. The committee is therefore perfectly positioned to test various economic risk scenarios and develop appropriate countermeasures.

Second, Taiwan has had in place a system of inbound and outbound investment screening for more than three decades. Conceived in the 1990s to avoid the hollowing out of the economy as companies relocated to China, the system was primarily geared to preserve competitiveness, with outbound investments to China, Hong Kong, and Macao falling under separate, stricter rules. This is in stark contrast to the approach of the EU and the United States, which consider security to be central.²¹ In April 2025, Taiwan's Legislative Yuan amended its outbound

regime, bringing national security into consideration for the first time. Beyond existing thresholds based on investment amount, transactions involving designated countries, regions, industries, or technologies must now obtain prior approval from MOEA, which can be denied in whole or in part, or subject to conditions, if national security risks or adverse economic development impacts are identified.²² While the reform was initially unpopular with the business community, it gained traction amid public anxiety about TSMC's \$100 billion expansion in Arizona, which many perceive as a blow to the island's industrial edge. Taiwan shows that even a relatively open economy can remain attractive despite strong investment safeguards that help preserve its competitiveness. The island also shows that, when needed, an open economy can adapt its rules relatively quickly.

Third, Taiwan uses its export control and investment promotion toolkit. In June 2025, the MOEA International Trade Administration added more than 600 foreign entities, including Huawei and SMIC, to its Strategic High-Tech Commodities list,²³ which requires Taiwanese exporters such as TSMC to secure government licenses before shipping covered items. And in early 2026, the MOEA, with the United States, designated the "Five Trusted Industry Sectors" (semiconductors, AI, military, security and surveillance, and next-generation communications)²⁴ as the focus of joint investment promotion. Export controls and investment promotion are common worldwide, but the Taiwanese distinction is that such measures are budgeted for, exercised, and tied to clearly identified scenarios.

Operationalizing Europe's Economic Security

Unlike Taiwan, which treats economic disruption as an imminent threat, the EU still primarily approaches economic security as a high-level strategy rather than as a set of practiced responses. The core elements of economic security—promoting key sectors, partnering with trusted economies, and protecting against coercion—are in place but are not embedded in operational frameworks that can be quickly activated under pressure. Instruments such as the Anti-Coercion Instrument (ACI), the International Procurement Instrument, the updated Foreign Direct Investment Screening Regulation agreed in December 2025, and the EU's trade-defense tools remain defensive and reactive in character. With unclear thresholds for action, slow procedures, and weak signaling, these tools do not meaningfully shape the behavior of potential coercers or their expectations about the EU's likely response, reducing their deterrent effect.

The ACI illustrates the problem. The European Commission has consistently emphasized that the instrument's primary objective is deterrence and that it "will be most successful if there is no need to use it."²⁵ However, such rhetoric works against its stated purpose. As of mid-2026, the ACI has not been triggered, though the idea has been floated several times, most recently in response to the dispute over Greenland with the United States. Without a clear indication of how and when it would be deployed, the ACI cannot pose a credible threat as a coordinated and immediate response, greatly diminishing its effect.

The same is true of the EU's investment-screening rules. Even after the December 2025 agreement to further harmonize the EU's foreign investment screening systems, final screening decisions remain

the responsibility of individual member states.²⁶ The updated screening framework therefore still lacks the predictability needed to avoid unnecessarily hampering investments while reliably alerting policymakers to genuine security risks.

In that sense, the EU's economic security concept remains largely a peacetime strategy and is out of step with current geopolitical realities. Taiwan's experience points to a more practical approach. Bridging this gap requires concrete scenario and contingency planning, with the Taiwan Strait as one of the core geographical areas of focus. Gray-zone disruptions, naval blockades, and open conflict should be met with predefined responses that can be activated quickly. This includes stockpiling, prioritizing critical sectors, stabilizing financial flows, and coordinating with the G7 and other trusted partners. The Commission's Economic Security Network and the proposed Council Working Group on Economic Security could provide the institutional backbone but only if member states translate intelligence into shared playbooks. Finding common ground can be achieved through joint exercises and economic security drills.

A more active posture also strengthens deterrence. It signals not only the ability to respond, but the readiness to do so under pressure. Crucially, deterrence depends on the capacity to absorb the economic fallout. The more prepared the EU is to manage a disruption, the more credible its response becomes. Taiwan's example shows that resilience is built not by writing strategies but by putting them into practice, automating certain steps, and preparing for all eventualities.²⁷ Without this shift, Europe risks having the right tools but lacking the speed and resilience needed to use them when it matters.

Endnotes

- ¹ Phillip Brown, Michael Ratner, Liana W. Rosen, and Clayton Thomas, "Iran Conflict and the Strait of Hormuz: Impacts on Oil, Gas, and Other Commodities" (Report R45281), Congressional Research Service, March 11, 2026. <https://www.congress.gov/crs-product/R45281>
- ² United Nations Development Programme Asia-Pacific, "Middle East military escalation could cost Asia-Pacific up to US\$299 billion", April 14, 2026. <https://www.undp.org/asia-pacific/press-releases/middle-east-military-escalation-could-cost-asia-pacific-us299-billion-undp>
- ³ Matthew P. Funaiolo, Brian Hart, David Peng, Bonny Lin, and Jasper Verschuur, "Crossroads of Commerce: How the Taiwan Strait Propels the Global Economy", Center for Strategic and International Studies, 2024. <https://features.csis.org/chinapower/china-taiwan-strait-trade/>
- ⁴ European Automobile Manufacturers' Association, "State of the EU Auto Industry – Full Year 2021", March 2022. https://www.acea.auto/files/economic_and_market_report-full-year_2021.pdf
- ⁵ Charlie Vest, Agatha Kratz, and Reva Goujon, "The Global Economic Disruptions from a Taiwan Conflict", Rhodium Group, December 14, 2022. <https://rhg.com/research/taiwan-economic-disruptions/>
- ⁶ Bloomberg Economics, "Xi, Biden and the \$10 Trillion Cost of War Over Taiwan", January 2024. <https://www.bloomberg.com/news/features/2024-01-09/if-china-invades-taiwan-it-would-cost-world-economy-10-trillion>
- ⁷ Michael Nakhiengchanh, "Taiwan enforces 'N-2 rule' on TSMC expansion in US", Taiwan News, December 18, 2025. <https://www.taiwannews.com.tw/news/6267804>
- ⁸ TrendForce, "TSMC N3 Tightens on AI Demand; Arizona 2nd Fab 3nm Volume Production in 2H27, Kumamoto in 2028", April 16, 2026. <https://www.trendforce.com/news/2026/04/16/news-tsmc-n3-tightens-on-ai-demand-arizona-2nd-fab-3nm-volume-production-in-2h27-kumamoto-in-2028/>
- ⁹ TrendForce, "TSMC 3nm Monthly Capacity May Hit 180K Wafers by 2026, Up Over 40% YoY on AI Demand", April 27, 2026. <https://www.trendforce.com/news/2026/04/27/news-tsmc-3nm-monthly-capacity-may-hit-180k-wafers-by-2026-up-over-40-yoy-on-ai-demand/>
- ¹⁰ Jeff Pao, "Rumored Japan photoresist ban sparks China's worst fears", Asia Times, November 27, 2025. <https://asiatimes.com/2025/11/rumored-japan-photoresist-ban-sparks-chinas-worst-fears/>
- ¹¹ European Commission, "Joint Communication on European Economic Security Strategy", Document 52023JC0020, June 20, 2023. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52023JC0020>. See also updates from [January 2024](#) and [December 2025](#).
- ¹² Jonathon Marek, "Better Ahead Than Red: US-Taiwan Cooperation for Non-PRC Tech Supply Chains", Global Taiwan Institute, September 17, 2025. <https://globaltaiwan.org/2025/09/better-ahead-than-red/>
- ¹³ Jonathan Harman, "Taiwan's Emerging Indigenous Drone Industry—An Overview", Global Taiwan Institute, February 11, 2026. <https://globaltaiwan.org/2026/02/tw-drone-production/>
- ¹⁴ The Economist, "Taiwan's bid to export drones free of Chinese parts is taking off", March 12, 2026. <https://www.economist.com/asia/2026/03/12/taiwans-bid-to-export-drones-free-of-chinese-parts-is-taking-off>
- ¹⁵ Hong-Lun Tiunn, Cathy Fang, Chun-Kuei Lai, Jenny Li, and Ru-Tung Elizabeth Sun, "Drones for Democracy: U.S.–Taiwan Cooperation in Building a Resilient and China-Free UAV Supply Chain", Research Institute for Democracy, Society and Emerging Technology, June 16, 2025. <https://dset.tw/en/research/drones-for-democracy-the-strategic-imperative-for-u-s-taiwan-uav-cooperation/>
- ¹⁶ Jane Rickards, "Taiwan's Drone Industry Take Off — but Can It Scale?", Taiwan Business Topics, April 20, 2026. <https://topics.amcham.com.tw/2026/04/taiwans-drone-industry-take-off-but-can-it-scale/>
- ¹⁷ Taiwan Excellence Drone International Business Opportunities Alliance, "About", 2026. <https://www.tediboa.com.tw/en/About>
- ¹⁸ Rebecca Kuo, "Taiwan's drone maker eyes DJI throne as US\$1.6 billion military contract looms", DigiTimes, October 9, 2025. <https://www.digitimes.com/news/a20251008PD223/taiwan-subsidiary-dji-military-demand.html>
- ¹⁹ Paddy Stephens, "Taiwan's drone industry: vertical take-off", Resilience Media, October 14, 2025. <https://resiliencemedia.co/taiwans-drone-industry-vertical-take-off/>
- ²⁰ Bonnie S. Glaser and Amanda Hsiao, "Taiwan's Push for Societal Resilience", German Marshall Fund of the United States, February 25, 2026. <https://www.gmfus.org/news/taiwans-push-societal-resilience>
- ²¹ Dah-Wei (David) Yih, "Rethinking Taiwan's Investment Security Strategy", Global Taiwan Brief 10, no. 9, May 7, 2025. <https://globaltaiwan.org/2025/05/rethinking-taiwans-investment-security-strategy/>
- ²² Tsung-Yuan Shen, Rachel Chen, and Effie Peng, "Taiwan's Cross-Border Semiconductor Controls: Export, Security and Investment Regulations", Asia Business Law Journal, January 29, 2026. <https://law.asia/taiwan-semiconductor-export-controls/>
- ²³ Ching-Fu Lin and Han-Wei Liu, "Silicon Statecraft: Alignment in Taiwan's Strategic Bet on US-Led Export Controls", The Diplomat, July 1, 2025. <https://thediplomat.com/2025/07/silicon-statecraft-alignment-taiwans-strategic-bet-on-us-led-export-controls/>
- ²⁴ Bryan Chuang, "Taiwan and US to jointly boost investments in five trusted industries", DigiTimes, March 6, 2026. <https://www.digitimes.com/news/a20260306PD215/taiwan-moea-semiconductors-security-investment.html>
- ²⁵ European Commission, "Questions and Answers: Anti-Coercion Instrument", 2026. https://policy.trade.ec.europa.eu/enforcement-and-protection/protecting-against-coercion/qa-regarding-anti-coercion-instrument_en

²⁶ Council of the European Union, "Foreign direct investment: Council and Parliament reached political agreement to improve FDI screening" (press release), December 11, 2025. <https://www.consilium.europa.eu/en/press/press-releases/2025/12/11/foreign-direct-investment-council-and-parliament-reached-political-agreement-to-improve-fdi-screening/>

²⁷ Ignacio García Bercero and Niclas Poitiers, "From Strategy to Doctrine: The Next Steps for European Economic Security", Bruegel, December 2, 2025. <https://www.bruegel.org/policy-brief/strategy-doctrine-next-steps-european-economic-security>

Preparing for Taiwan

Economic Coordination Must Begin Before a Crisis

By Jacqueline Ramos

Introduction

Policy debates about Taiwan tend to rely on a familiar frame: a bilateral contest between the United States and China, with Europe often viewed as peripheral to the core strategic competition. Militarily, that framing is understandable. Economically, it is increasingly detached from how a Taiwan crisis would unfold.

A crisis in the Taiwan Strait would reverberate far beyond the Pacific. Europe's role in global trade, technology regulation, financial markets, and advanced industrial supply chains would make it an essential participant in any coordinated response. The United States and Europe would likely need to coordinate export controls, sanctions, financial restrictions, and technology measures under severe time pressure.

This paper argues that the central challenge in a Taiwan contingency is not whether the United States and Europe possess such economic tools, but whether they have built the political, institutional, and private-sector coordination needed to deploy them before a crisis begins. Drawing on Europe's response to Russia's full-scale invasion of Ukraine, this paper shows that economic coordination is difficult to assemble once markets, firms, and governments begin reacting simultaneously. Effective economic coordination must be built in advance if it is to support credible economic deterrence. This paper also explains why Europe's economic interests and institutional authorities make it indispensable to any coordinated response and identifies steps to strengthen transatlantic economic preparedness.

What Europe's Response to Russia Revealed About Economic Deterrence

Europe's response to Russia's 2022 invasion of Ukraine showed that advanced economies retain enormous collective economic leverage when acting together, from immobilizing roughly \$300 billion in Russian central-bank assets to removing major Russian banks from SWIFT and sharply restricting access to advanced semiconductors, aviation components, and dual-use technologies.¹ European governments also reduced dependence on Russian pipeline gas at a pace many policymakers had previously considered politically and economically unrealistic. Before the invasion, Russia supplied roughly 40% of the European Union's natural gas imports. By 2023, that figure had fallen to roughly 8%.²

The West clearly possessed enormous economic leverage. Yet the opening stages of the crisis also revealed how difficult coordinated action becomes once events begin moving quickly. European governments broadly agreed on the strategic imperative after Russia's invasion, but translating political consensus into coordinated economic action still proved slower and more difficult than many policymakers expected. EU sanctions packages required negotiations across twenty-seven governments with different legal authorities, trade exposure, domestic political pressures, and threat perceptions. Those negotiations unfolded even as governments were identifying vulnerabilities that extended well beyond energy to shipping insurance,

industrial commodities, fertilizer markets, financial exposure, and specialized manufacturing inputs.

Those frictions were not simply bureaucratic. They reflected genuine differences in economic dependencies, political tolerance for economic pain, and assumptions about escalation risk. Some governments viewed rapid sanctions expansion as strategically necessary despite economic costs, while others were more concerned about inflation, energy stability, and domestic political backlash.³ Maintaining cohesion therefore required continual negotiation across allied capitals.

Before the invasion, many policymakers believed Europe's dependence on Russian energy imposed hard constraints on the scale and speed of possible economic measures. The crisis challenged those assumptions. Europe reduced Russian pipeline gas imports far more rapidly than many observers had expected, but doing so required sustained political coordination, alternative sourcing arrangements, domestic support measures, and extensive diplomacy across allied governments.

Governments were not the only actors shaping the pace of the economic response. In many cases, the private sector moved faster than governments themselves. Financial institutions, insurers, logistics firms, commodity traders, and multinational corporations rapidly reassessed operational and legal risk. Firms such as Maersk, BP, Shell, and major global financial institutions began suspending operations or reevaluating commercial ties within days of the invasion, in many cases before allied governments had fully coordinated their response.⁴ At the same time, markets repriced risk almost immediately, even as governments were still negotiating the scope, sequencing, and implementation of sanctions packages and export-control measures.

The crisis exposed an uncomfortable reality for policymakers. Governments do not fully control the tempo of modern economic crises once markets begin repricing risk. Firms respond to anticipated political direction, legal uncertainty, reputational concerns, insurance pressures, and market volatility long before governments finalize coordinated responses. Economic deterrence therefore depends not only on government decision-making, but also on whether governments and major private-sector actors can anticipate one another's likely responses before formal policy decisions are complete.

Maintaining transatlantic cohesion during Russia's aggression against Ukraine has also required constant diplomatic management across the G7, the EU, NATO, foreign ministries, treasury ministries, export-control authorities, and allied capitals. Governments have coordinated intelligence disclosures, synchronized sanctions announcements, aligned public messaging, and engaged in continual consultations to keep allies moving in the same direction politically as well as economically. That cohesion has required careful political management, particularly as the economic costs of sanctions and energy disruption became more visible domestically. Alliance management was not simply a diplomatic requirement; it became a central component of economic strategy itself.

Deterrence depends partly on expectations. If governments appear divided over costs, sequencing, or escalation management, adversaries are more likely to conclude that economic coalitions will weaken under pressure. The experience in Ukraine has revealed a gap between possessing economic tools and being prepared to deploy them quickly and coherently under severe time pressure. The lesson was not that coordinated economic action was impossible. Rather, it was that assembling and sustaining that coordination under an active crisis required far more

political, institutional, and commercial alignment than many policymakers had anticipated.

Taiwan and the Limits of Bilateral Thinking

The Ukraine experience also demonstrates why Taiwan would present a far more demanding coordination challenge. A Taiwan contingency would unfold under far tighter timelines and create significantly broader market disruption. Russia's invasion of Ukraine followed months of visible military buildup, escalating warnings, and extensive public intelligence disclosures. A Taiwan crisis could evolve much faster, particularly if triggered through coercive measures short of full-scale invasion, including maritime blockades, cyberattacks, gray-zone escalation, or episodic disruptions to commercial shipping. Governments could face immediate market turmoil while still debating the nature and scope of the crisis itself.

The nature of Taiwan-related economic exposure is also fundamentally different from Europe's pre-2022 energy dependence on Russia. Taiwan accounts for more than 90 percent of leading-edge chip manufacturing and over 60 percent of global foundry revenue.⁵ Yet Taiwan's role in the semiconductor ecosystem is not simply a matter of manufacturing volume. Advanced semiconductor production depends on a tightly integrated system involving US chip-design firms, Dutch lithography technology, Japanese materials and chemicals, Taiwanese fabrication capacity, and globally distributed downstream manufacturing.⁶ European firms and regulators are deeply embedded in this ecosystem, particularly through Dutch lithography expertise, industrial machinery, chemicals, and manufacturing sectors vulnerable to semiconductor disruption. In

that sense, a Taiwan conflict would create a more concentrated and technologically integrated shock to Europe's technology supply chain than the energy shock Europe faced after Russia's full-scale invasion of Ukraine.

This is not simply a supply-chain vulnerability. It reflects a concentration of technological capacity with few near-term substitutes and no realistic path to rapid replacement under crisis conditions. This fundamentally changes the structure of strategic risk. A disruption in the Taiwan Strait would likely affect not only semiconductor availability, but also shipping insurance, maritime routing, container pricing, financial markets, industrial production, and broader commercial confidence across the Indo-Pacific. Unlike Russia's invasion of Ukraine, where some sectors experienced staggered effects over time, a Taiwan crisis would likely generate simultaneous disruptions across multiple economic systems.

Bloomberg Economics estimated that a conflict over Taiwan could erase roughly 10% of global GDP, exceeding the combined economic shock of the global financial crisis and the COVID-19 pandemic.⁷ Other analyses have similarly warned that major disruption in the Taiwan Strait would generate cascading effects across global trade flows and industrial production.⁸

Under these conditions, governments would have even less time to sequence economic decisions. Shipping firms, insurers, semiconductor companies, financial institutions, and multinational manufacturers would begin repricing risk almost immediately, potentially reshaping commercial realities before allied governments had reached political consensus on response measures. As in the Ukraine crisis, many of the most consequential commercial decisions would likely be made before governments had finalized a coordinated response.

Europe is already deeply embedded in these dynamics. EU-China trade has remained above €700 billion annually in recent years despite growing European concern about strategic dependencies and repeated calls for de-risking.⁹ China also remains tightly integrated in European industrial supply chains, including rare earths, batteries, pharmaceuticals, clean energy technologies, and critical manufacturing inputs. European governments and EU institutions, meanwhile, play central roles in export controls, technology regulation, sanctions enforcement, investment screening, and financial access, making Europe an essential participant in any coordinated economic response to a Taiwan crisis.

At the same time, European governments do not approach China from identical political or economic positions. Exposure varies significantly across sectors and member states, as do domestic political calculations surrounding trade, industrial competitiveness, and strategic risk.¹⁰ Some governments have moved more aggressively toward de-risking strategies, while others remain more cautious about measures that could generate economic retaliation or commercial disruption. Those differences at the national level can also complicate cohesion within EU institutions themselves, particularly when member states hold differing views on trade, industrial policy, and economic risk.

Many policy discussions still treat European coordination as something to be organized after a crisis begins, rather than a prerequisite for credible economic deterrence. That assumption underestimates how quickly commercial decisions, market reactions, and political constraints would accumulate long before governments would have time to build coordination from scratch.

Treating Taiwan as a bilateral issue does not simplify planning. It postpones the harder task of aligning

governments, regulators, EU institutions, and private-sector actors before crisis conditions emerge. Europe is not a peripheral player in the financial and industrial dimensions of a Taiwan crisis. It is already part of the system. The problem is that policy planning across European governments and EU institutions has not fully caught up with Europe's central role in a Taiwan contingency.

Building Economic Coordination Before Crisis

Building economic coordination before a crisis requires sustained political, institutional, and commercial preparation. The challenge is not identifying the necessary mechanisms but overcoming the political and institutional barriers that have left EU-level coordination difficult to organize and comparable national-level planning uneven or absent. To achieve this, a more structured framework for US-EU economic contingency planning related to Taiwan is needed, including regular engagement with relevant EU institutions alongside national governments. Quiet coordination among foreign ministries, finance ministries, export control authorities, trade officials, and regulatory agencies would improve readiness before a crisis emerges.

Given the varying levels of economic dependence on China across Europe, these discussions should also include targeted bilateral consultations with the most exposed allied governments. Stronger coordination among major European capitals would make broader EU-level alignment more sustainable under crisis conditions.

Joint economic contingency exercises focused on sanctions coordination, export controls, shipping disruptions, financial instability, and semiconductor

supply shocks would significantly improve allied preparedness. Existing coordination mechanisms are not designed to manage simultaneous disruptions across trade, finance, logistics, and technology sectors at the scale of a Taiwan contingency. Structured exercises would help identify legal bottlenecks, sequencing problems, information gaps, and commercial vulnerabilities before governments are forced to manage them during a live crisis.

Routine contingency exercises should not themselves become politically controversial. Conducting planning exercises does not predetermine future policy decisions; it simply strengthens institutional readiness should governments need to act under compressed timelines. Military planners routinely stress-test operational readiness before crises emerge, and economic deterrence requires a similar degree of preparation. Governments should not assume coordination mechanisms will function smoothly if first tested during an active Taiwan crisis.

More structured and sustained engagement with major private-sector actors is also necessary before a crisis emerges. Financial institutions, logistics firms, semiconductor companies, and other major multinational corporations will shape economic outcomes from the earliest stages of any Taiwan contingency. In practice, many of the initial economic decisions in a Taiwan crisis would not be made by governments at all, but by firms reacting to rapidly changing risk calculations. More structured engagement would improve information sharing, reduce uncertainty driven by overreaction, and provide firms with clearer expectations regarding likely government responses under crisis conditions.

Allies should also align legal and regulatory authorities in advance wherever possible. Europe's response to Russia demonstrated how differing legal authorities, domestic procedures, and institutional processes

can slow coordination even among close allies. That preparation will be particularly important in areas where allied governments possess different legal authorities, regulatory frameworks, or thresholds for economic escalation.

Allies would also benefit from more coordinated diplomatic and public signaling strategies before a crisis occurs. Coordinated public messaging, synchronized announcements, and clearer signaling on sequencing would enhance credibility during the early stages of a contingency. Markets and firms react not only to formal policy measures, but also to perceptions of whether governments appear aligned or divided, decisive or uncertain. The objective is straightforward: Reduce uncertainty, improve alignment, and strengthen deterrence credibility before crisis timelines compress.

Conclusion

The allied response to Russia's invasion of Ukraine demonstrated that coordinated economic pressure can impose severe costs over time. It also revealed how difficult coalition management becomes once markets, firms, regulators, and governments begin reacting simultaneously under crisis conditions.

In a Taiwan scenario, those same pressures would emerge far more quickly and simultaneously. Timelines would be shorter, economic disruption broader, and market reactions faster. Governments, including European governments with deep trade relationships with Taiwan and China, would face simultaneous demands across trade, finance, technology, shipping, and industrial supply chains almost immediately.

That reality carries a significant implication for policymakers: Economic deterrence cannot be improvised once a crisis begins. While governments debate sequencing, authorities, and coordination mechanisms, commercial actors may already be reshaping the strategic environment themselves. Taiwan therefore presents not simply a military contingency or a bilateral US-China problem. A crisis in the Strait would test whether the United States, Europe, and their partners have built the political, economic, and institutional foundations necessary for coordinated action before events overtake them.

Endnotes

¹ Reuters, "Russia could concede \$300 billion in frozen assets as part of Ukraine war settlement, sources say", February 21, 2025. <https://www.reuters.com/world/europe/russia-could-concede-300-bln-frozen-assets-part-ukraine-war-settlement-sources-2025-02-21/>; Council of the European Union, "Timeline – EU restrictive measures against Russia over Ukraine", 2025. <https://www.consilium.europa.eu/en/policies/sanctions-against-russia/timeline-sanctions-against-russia/>; European Commission, "EU sanctions against Russia following the invasion of Ukraine", 2025. https://commission.europa.eu/topics/eu-solidarity-ukraine/eu-sanctions-against-russia-following-invasion-ukraine_en

² Ugnė Keliauskaitė, Ben McWilliams, Giovanni Sgaravatti, and Georg Zachmann, "European natural gas imports tracker" [Dataset], Bruegel, n.d. <https://www.bruegel.org/dataset/european-natural-gas-imports>; European Commission, "REPowerEU", 2025. https://commission.europa.eu/topics/energy/repowereu_en

³ John O'Donnell, "EU Unity over Russia Sanctions Falters as Europe's Economy Wilts", Reuters, December 19, 2022, <https://www.reuters.com/markets/europe/eu-unity-over-russia-sanctions-falters-europes-economy-wilts-2022-12-16/>; Francesco Guarascio and John Chalmers, "EU's Toughest Russia Sanctions Yet Snag on Worries over Oil Ban", Reuters, May 4, 2022, <https://www.reuters.com/world/europe/eu-lay-out-new-sanctions-russia-targeting-oil-imports-2022-05-04/>; European Council, "European Council Conclusions on Ukraine, 30 May 2022", May 31, 2022, <https://www.consilium.europa.eu/en/press/press-releases/2022/05/31/european-council-conclusions-on-ukraine-30-may-2022/>

⁴ Yale Chief Executive Leadership Institute, "Over 1,000 Companies Have Curtailed Operations in Russia – But Some Remain", Yale School of Management, n.d. <https://som.yale.edu/story/2022/over-1000-companies-have-curtailed-operations-russia-some-remain>

⁵ International Trade Administration, "Taiwan – Semiconductors including chip design for AI", December 1, 2025. <https://www.trade.gov/country-commercial-guides/taiwan-semiconductors-including-chip-design-ai>

⁶ Tripp Mickle, "The Looming Taiwan Chip Disaster That Silicon Valley Has Long Ignored", The New York Times, February 24, 2026. <https://www.nytimes.com/2026/02/24/technology/taiwan-china-chips-silicon-valley-tsmc.html>; Semiconductor Industry Association, "2024 State of the US Semiconductor Industry", October 2024. https://www.semiconductors.org/wp-content/uploads/2024/10/SIA_2024_State-of-Industry-Report.pdf; Akhil Thadani and Gregory C. Allen, "Mapping the Semiconductor Supply Chain: The Critical Role of the Indo-Pacific Region", Center for Strategic and International Studies, May 30, 2023. https://csis-website-prod.s3.amazonaws.com/s3fs-public/2023-05/230530_Thadani_MappingSemiconductor_SupplyChain.pdf

⁷ David Stringer, "War over Taiwan Would Cost World Economy \$10 Trillion", Bloomberg Newsletter, January 9, 2024. <https://www.bloomberg.com/news/newsletters/2024-01-09/war-over-taiwan-would-cost-world-economy-10-trillion-big-take>

⁸ Charlie Vest, Agatha Kratz, and Reva Goujon, "The Global Economic Disruptions from a Taiwan Conflict", Rhodium Group, December 14, 2022. <https://rhg.com/research/taiwan-economic-disruptions/>; Ben Bland, "A Taiwan crisis would cause far more global economic damage than Strait of Hormuz disruption", Chatham House, April 22, 2026. <https://www.chathamhouse.org/2026/04/taiwan-crisis-would-cause-far-more-global-economic-damage-strait-hormuz-disruption>; Center for Preventive Action, "Confrontation Over Taiwan", Council on Foreign Relations Global Conflict Tracker, updated July 14, 2026. <https://www.cfr.org/global-conflict-tracker/conflict/confrontation-over-taiwan>

⁹ Gabriel Gavin and Carlo Martuscelli, "EU Commission plans new squeeze on Chinese trade", Politico, May 15, 2026. <https://www.politico.eu/article/eu-commission-reduce-economic-dependence-chinese-trade-plan/>; European Commission, "EU trade relations with China", 2025. https://policy.trade.ec.europa.eu/eu-trade-relationships-country-and-region/countries-and-regions/china_en

¹⁰ Ryan Woo, Xiuhao Chen, and Yukun Zhang, "China's economy tsar invites EU trade chief to jointly resist tariff threats", Reuters, March 27, 2025. <https://www.reuters.com/world/china-hopes-europe-will-make-rational-choice-transatlantic-alliance-shifts-2025-03-27/>

Taiwan Needs an Asylum Law

Refugee protection as security policy

By Colleen Scribner

Since ending martial law in 1987, Taiwan has gradually transformed into one of Asia's most resilient democracies. It has also become a rights-respecting society on the front lines of geopolitical competition in the Indo-Pacific. Freedom House consistently rates Taiwan "free" in its Freedom in the World and Freedom on the Net reports due to its vibrant, competitive democratic system and protection of civil liberties.¹

However, Taiwan lacks a formal system that allows refugees—defined by UNHCR as those who are "unable or unwilling to return to their country of origin due to a well-founded fear of persecution"—to seek asylum.² This gap in Taiwan's democratic architecture is increasingly consequential as space for political dissent and social organizing has narrowed across the Indo-Pacific as a result of shrinking civic space in Southeast Asia, sustained repression in China, and a crackdown in Hong Kong, among other factors. Taiwan, by virtue of its geography and political identity, is a natural destination for individuals, including activists, journalists, religious minorities, and political dissidents, fleeing political persecution and growing authoritarianism in neighboring jurisdictions. In the absence of an asylum framework, these individuals often endure a lack of legal protection; vulnerability to exploitation and social marginalization; limited access to social services such as healthcare, housing, and education; lack of employment access; and the persistent risk of refoulement, detention, or prolonged insecurity.

Taiwan's inability to provide a clear legal pathway for asylum seekers is a human rights deficiency and a strategic vulnerability. A formal asylum law and system would strengthen Taiwan's national security by shoring up its democratic credibility, deterrence posture, coordination with like-minded countries, and domestic governance practice.

A Fragmented and Discretionary System

Taiwan has debated refugee legislation for nearly two decades. Since the first proposal in 2005, Democratic Progressive Party (DPP) and Kuomintang (KMT) party members have proposed more than 10 versions of a draft Refugee Act (難民法草案) to the Legislative Yuan³. A 2016 draft passed its first reading, but progress then stalled⁴. It established procedures for refugee applications, review mechanisms, temporary residency, applicant rights, and grounds for rejection (all under Ministry of Interior's oversight). It also adopted a broader definition of refugee status than the 1951 Refugee Convention by including individuals displaced by war and natural disasters.

In the absence of a formal asylum law, Taiwan relies on a patchwork of legal authorities, administrative discretion, and case-by-case "special projects". The result is a set of parallel pathways with different rules, timelines, and outcomes depending on the applicant's origin.

For applicants from China, cross-strait legal frameworks, not refugee law, govern cases.⁵ Applicants petition Taiwan's National Immigration Agency (NIA) and may then undergo a discretionary "special project" review process involving the Mainland Affairs Council (MAC) if their entry is deemed legal. Approval hinges on a narrow and highly subjective set of criteria centered on political sensitivity and strategic values, such as whether the individual has made contributions to Taiwan's national interests, possesses politically valuable information, holds symbolic status, or can demonstrate a credible risk of persecution tied to democratic activism. The process is neither swift nor predictable. Successful applicants may receive temporary residency, but only after extended review periods that, in some cases, stretch into years. Historically, some Chinese dissidents waited over a decade to secure stable legal status.⁶ For those who have entered Taiwan irregularly, the situation is even more precarious. They may endure detention, fines, or repatriation unless civil society actors intervene as guarantors.

Asylum seekers from Hong Kong and Macao follow a separate but similarly opaque and discretionary process, with final decisions elevated to the Executive Yuan and an interagency review to determine if residency will be granted.⁷ A dedicated humanitarian initiative for Hong Kong protesters provides more structured intake and limited social and medical support, but outcomes still depend on interagency discretion rather than on clear legal standards.⁸

Pathways are even less defined for applicants from other regions. They may theoretically receive temporary documentation allowing them to remain in Taiwan while their cases are under review. In practice, however, this process has stalled and produced no confirmed or rejected cases, leaving individuals in prolonged legal limbo without access to work, services, or stable housing.

Across all refugee categories, access to case review and social services is inconsistent, transparency is limited, timelines are unpredictable, and legal status during review is weak or nonexistent. This creates openings for politicization, weak oversight of approved cases, and uneven risk assessment.

Strategic Competition and Domestic Vulnerabilities

Democratic credibility in cross-strait competition

Taiwan's government has increasingly framed the island as a frontline democracy resisting authoritarian pressure in the Indo-Pacific. This identity is not symbolic. It shapes Taiwan's relationships and engagement with partners in Europe and North America and contributes to efforts to strengthen deterrence against coercion and intervention from Beijing. Taiwan's political credibility as a democratic beacon undergirds its deterrence posture, but its lack of an asylum system undercuts this and is a gap in Taiwan's democratic architecture.

This matters in the context of cross-strait competition. Beijing promotes aspects of its governance approach and authoritarian development model as an alternative to liberal democracy. In that environment, Taiwan's response cannot rely on informal, opaque processes. A rules-based asylum framework would reinforce the contrast Taiwan seeks to draw between Beijing's approach to governance and a more accountable and rights-respecting political system. While the Chinese government routinely restricts access to information, criminalizes activism, silences activists and marginalized communities, and limits press freedom, democratic systems distinguish themselves by providing legal

protection to individuals facing persecution for exercising their human rights and fundamental freedoms. Providing refuge for political dissidents, journalists, and activists is one of the most visible ways democracies differentiate themselves from authoritarian regimes. It transforms abstract human rights commitments into policies that protect those in need and rule-of-law initiatives.

The absence of formal asylum law also creates constraints on cooperating with democratic partners due to the diplomatic and legal uncertainty that can arise from the absence of a legal framework. As Taiwan seeks to deepen ties with Europe and other democracies, the lack of a coherent refugee system appears increasingly out of step with its broader positioning.

National security and risk management

The most persistent argument against establishing an asylum system in Taiwan is security. Those opposing such a system see a risk that hostile actors could exploit refugee pathways to enter and operate within the island. But the current ad hoc system may already allow threats to slip through inconsistent screening while denying legitimate applicants protection due to overly cautious or opaque decision-making. It also allows for the politicalization of cases.

A formal asylum framework would improve security screening by establishing clear, standardized procedures for background checks, interagency coordination, intelligence sharing, and case review. It would enhance security outcomes and institutional accountability. Defined timelines and criteria would reduce uncertainty and increase transparency.

Regularized legal status would also improve long-term oversight. Individuals left in prolonged legal limbo are vulnerable to exploitation and coercion, including

transnational repression by authoritarian governments that target dissidents abroad through surveillance, intimidation, and information operations. Such individuals are also less likely to integrate in stable ways that bolster social cohesion.

Lessons from Abroad

Europe's response to Russia's full-scale invasion of Ukraine demonstrated that asylum policy can function as a humanitarian and human rights instrument, and a tool of geopolitical signaling.

In 2022, the EU activated the Temporary Protection Directive, granting millions of displaced Ukrainians immediate access to residency, work authorization, and social services in member states.⁹ The decision reflected humanitarian concerns but also communicated political resolve. European governments were prepared to operationalize their commitment to defending democratic societies against authoritarian aggression.

Taiwan operates under different constraints. It is not part of a regional bloc, lacks formal recognition in many international institutions, and consequently cannot rely on agencies such as the UNHCR. Still, an asylum system could serve similar strategic functions by enabling quiet coordination with democratic partners through information sharing, coordinated resettlement pathways, or joint approaches to high-risk cases.

Provoking the Dragon?

Concern about Beijing's reaction shapes Taiwan's approach to asylum policy, particularly for applicants

from China, Hong Kong, and Macao. The issue is politically sensitive because Taiwan's constitution establishes a legal framework that treats residents of those three territories differently from others, reflecting the unresolved status of cross-strait sovereignty claims.¹⁰ Policymakers worry that creating formal refugee categories for individuals from China, Hong Kong, or Macao could have implications for cross-strait relations by implicitly acknowledging that these individuals are fleeing a "foreign" political system. In other words, Beijing could interpret classifying applicants from these territories as refugees as a step toward formal independence for Taiwan, thereby escalating cross-strait tensions.

China has not made public comments on Taiwan's asylum system, but it sharply criticized President Tsai Ing-wen's call to provide humanitarian assistance to activists during protests in Hong Kong in 2019. Beijing warned the Tsai administration to "immediately withdraw their black hands from Hong Kong, cease meddling in Hong Kong affairs, stop condoning and harboring violent radicals, and end any actions that would undermine cross-strait relations".¹¹

That response shows that Taiwan's undertaking a more modest and ad hoc approach to asylum seekers from Hong Kong has not insulated it from criticism. A more formalized system would not eliminate Chinese political pressure, but it would place Taiwan on firmer ground when responding to it. Pointing to a structured asylum framework grounded in clearly defined legal criteria would allow Taipei to reduce public skepticism and erode Beijing's ability to control the narrative by dispelling any sense that individual cases are politically motivated.

Recommendations

A comprehensive asylum framework would close a long-standing human rights gap and strengthen Taiwan's national security and institutional resilience. The island's 2016 Refugee Act draft provides a workable foundation for such a framework. Taipei should now refine the legislation and prioritize its passage. Separate, subsequent legislation should address the different risks and profiles of asylum seekers from China, Hong Kong, and Macao.

The 2016 draft should be modified to incorporate the following:

- **Formalize the role of civil society.** Civil society organizations already perform core functions within Taiwan's de facto asylum system. These include providing legal assistance, financial support, and housing, in addition to serving occasionally as guarantors for applicants navigating immigration processes. Policymakers should integrate these actors into the formal system (beyond existing mentions of them in Article 5 and Article 9 regarding the review process and measures for a high applicant numbers) by giving them designated roles in applicant support services, structured funding mechanisms to sustain their ability to provide legal and other forms of support, and government coordination protocols.
- **Create emergency and temporary protection pathways.** Taiwan's experience with asylum seekers from Hong Kong demonstrates the need for rapid-response mechanisms. Millions of Hong Kongers participated in 2019 in protests against a proposed extradition bill that would have allowed individuals to be transferred

to mainland China for trial. Protesters feared that the measure would undermine judicial independence and expose political dissidents to prosecution. As protests were met with arrests, police crackdowns, and, ultimately, the imposition of Beijing's 2020 National Security Law, activists, journalists, and others sought refuge abroad, including in Taiwan. The speed at which conditions deteriorated in Hong Kong demonstrates the need for government to have pathways that can provide protection to individuals affected by human rights crises. A formal asylum framework should include provisions for temporary or emergency protection status, allowing individuals at immediate risk to enter and remain in Taiwan while their cases are processed. These provisions could take the form of humanitarian visas or expedited review channels tied to specific events such as political crackdowns or large-scale repression.

- **Institutionalize coordination with democratic partners.** Taiwan's diplomatic constraints limit its participation in formal international refugee systems, but they do not preclude cooperation with democratic partners. This could include information sharing and coordination on high-risk cases, collaboration on response to transnational repression, or complementary resettlement arrangements.
- **Strengthen inclusion and protection of high-risk applicants in subsequent legislation.** Taiwan should first pass legislation that would apply to refugees from places other than China. Applicants from politically sensitive jurisdictions—China, Hong Kong, and Macao—should be dealt

with in subsequent, separate legislation. (The 2016 Refugee Act draft did not cover them.) Applicants from these three territories face distinct risks including surveillance, coercion, and retaliation against family members, and therefore pose unique challenges that require a high level of scrutiny. Taiwan's asylum system should account for these factors and strengthen inclusion and protection of high-risk applicants by enhancing confidentiality protections, secure case-handling procedures, and safeguards against transnational repression.

Conclusion

Asylum policy should be seen part of the architecture that sustains Taiwan's resilience. Done properly, a comprehensive asylum framework would close a persistent human rights gap while strengthening Taiwan's democratic narrative and broader national security framework. A transparent system could improve vetting, reduce ambiguity in decision-making, and mitigate security risks associated with unmanaged or opaque inflows. It would also align with international democratic norms, reinforcing Taiwan's role as a credible partner in global conversations on rights and governance. Until a policy is formalized, Taiwan's lack of an asylum law remains an institutional vulnerability.

Endnotes

¹ Freedom House, "Taiwan". <https://freedomhouse.org/country/taiwan>

² United Nations High Commissioner for Refugees, "Who we protect: Refugees". <https://www.unhcr.org/about-unhcr/who-we-protect/refugees>

³ Kai-Xuan Lin, "我國難民法立法之研究" [A Study on the Legislation of Refugee Law in Taiwan], Graduate Institute of National Development, National Taiwan University, July 28, 2018. <https://www.airitilibrary.com/Article/Detail/U0001-3011201814565100>

⁴ Ministry of the Interior, Republic of China (Taiwan), "難民法草案" [Refugee Act Draft], July 14, 2016. https://ws.moi.gov.tw/001/Upload/OldFile/Act_file/難民法草案%20條文對照表.PDF; Lin Shu-han, "從反送中到俄烏戰爭，在立院卡關17年的「難民法」為何遲遲不實現?" [From the anti-extradition to the Russia-Ukraine war, why has the "Refugee Law" that has been stuck in the Legislative Yuan for 17 years not been realized?], The News Lens, March 17, 2022. <https://www.thenewslens.com/article/164131>

⁵ Mainland Affairs Council, "Act Governing Relations between the People of the Taiwan Area and the Mainland Area", Laws & Regulations Database of The Republic of China (Taiwan), as amended June 8, 2022. <https://law.moj.gov.tw/ENG/LawClass/LawAll.aspx?pcode=Q0010001>

⁶ ShangGuan Luan, "中國籍政治難民在台灣：朝著民主自由「投誠」後，卻依舊無處容身" [Chinese Political Refugees in Taiwan: Nowhere to Call Home After "Defecting" to Democracy and Freedom], The News Lens, April 25, 2024. <https://www.thenewslens.com/article/201861>

⁷ Mainland Affairs Council, "Act Governing Relations with Hong Kong and Macao", Law & Regulations Database of The Republic of China (Taiwan), January 12, 2022. <https://law.moj.gov.tw/ENG/LawClass/LawAll.aspx?pcode=Q0010003>; Mainland Affairs Council, "Enforcement Rules of the Act Governing Relations with Hong Kong and Macao", Law & Regulations Database of The Republic of China (Taiwan), January 11, 2016. <https://law.moj.gov.tw/ENG/LawClass/LawAll.aspx?pcode=Q0010004>

⁸ Taiwan Association for Human Rights, "從不存在到不被肯認的存在：2019年後香港庇護機制在台灣的演進與限制" [From Nonexistence to Unrecognized Existence: The Evolution and Restrictions of Hong Kong's Asylum Mechanism in Taiwan After 2019], January 22, 2026. <https://www.tahr.org.tw/news/3835/>

⁹ European Commission, "Migration and asylum—Temporary protection", April 30, 2026. https://home-affairs.ec.europa.eu/policies/migration-and-asylum/asylum-eu/temporary-protection_en

¹⁰ National Assembly, Republic of China (Taiwan), "Constitution of the Republic of China: Main Text", Office of the President, as revised August 23, 2004. <https://english.president.gov.tw/page/94>

¹¹ Wang Siyu, "马晓光：民进党当局在近期香港事态中扮演了极不光彩的角色" [Ma Xiaoguang: The DPP authorities have played an extremely disgraceful role in the recent events in Hong Kong], Taiwan.cn, September 11, 2019. http://www.taiwan.cn/taiwan/jsxw/201909/t20190911_12200636.htm

Why Taiwan and the EU Should Align on Drones

and Why They Should Do It Upstream

By Ulf Steindl

From interstate conflicts in Ukraine and the Persian Gulf to irregular intrastate warfare in the Sahel or Myanmar, unmanned systems have become a central part of contemporary warfare. Armed forces worldwide are scrambling to learn the lessons of the Russia-Ukraine War, where a new type of attritional drone warfare is being pursued. Warfare depends on context and is shaped by the interaction of the warring parties, geography, industrial capacity, technology, and the particular political objectives being pursued. Nevertheless, current trends suggest that unmanned systems will remain relevant to warfare for the foreseeable future. The attritional nature of drone warfare also underscores the need to ensure scalability and resilience for the drone supply chain. This has direct implications for Taiwan, where the imbalance between Beijing and Taipei likewise demands an asymmetric defense approach that aims to exploit the opponent's vulnerabilities and prioritizes low-cost capabilities. Unmanned systems are set to play an important role for the deterrence-by-denial "porcupine" strategy of making an invasion prohibitively costly, and in pursuing underlying asymmetric defense concepts. Unmanned aerial vehicles (UAVs) already are foreseen to play a critical role in each of the three defense phases—force protection, littoral dominance, and beachhead neutralization—defined by Taiwan's Overall Defense Concept, a layered asymmetric defense strategy developed to oppose an invasion.¹

Ukraine's defensive war highlights the potentially immense demand for systems that can continue

to function under attritional conditions, which such asymmetric strategy requires. In 2025, Ukrainian UAV production is estimated to have reached between 4 and 4.5 million units, including more than 2 million first-person-view (FPV) UAVs.² Production numbers for unmanned vehicles on the ground (UGV), on the water surface (USV), and underwater (UUV) are significantly lower but likewise growing. Ukraine's domestic industry produced approximately 15,000 UGVs in 2025,³ and the Ukrainian Armed Forces reported more than 21,000 UGV missions in the first quarter of 2026, which by March represented a threefold increase since November 2025.⁴ Production numbers for maritime drones are less clear, but their employment in the war has been significant. By early 2026, Ukraine's Ministry of Defense estimated that approximately 30% of Russia's Black Sea Fleet combat assets had been destroyed or seriously damaged. Aerial and maritime drones played a crucial role in this campaign, forcing the fleet to withdraw from Sevastopol to Novorossiysk, where it remains under siege-like circumstances.⁵ This lesson carries particular weight for Taiwan, where the maritime domain is not just one theater but central to the entire defense of the island. USVs and UUVs would likely play a much more important role in Taiwan's littoral defense, while UGVs could take an important role during the beachhead neutralization phase.

Unlike Ukraine, which was compelled to develop its drone warfare capabilities in an intense learning and adaptation cycle and has had to set up drone production under wartime conditions, Taiwan and

EU member states can develop and scale these capabilities before a crisis emerges. Considerable focus thus lies on scaling production, expanding resilient supply chains, and keeping pace with the rapid innovation cycle made visible in Ukraine.

The Peacetime Conundrum: Scaling Production for Future Contingencies

Between 2024 and 2025, Taiwanese UAV production grew from 10,000 to 120,000 units per year. In the first two months of 2026 alone, more than 85,000 units were exported—a 35-fold year-on-year growth.⁶ These production numbers represent a noteworthy accomplishment for a peacetime economy but are nonetheless dwarfed by the usage of drones in the Russian-Ukraine War. Although Taiwan's armed forces intend to procure 200,000 units by 2033, the opposition-controlled Legislative Yuan has yet to provide funding.⁷ Even this procurement ambition is considerably lower than Ukraine's approximate monthly use of 270,000 UAVs in early 2026.⁸

Armed forces cannot sustain such an immense procurement effort during peacetime, but governments need to ensure that industry has the scalability to address demand during a conflict. Considering that Taiwan cannot rely on imports during a contingency, when they would be highly vulnerable to interdiction, a much higher degree of self-sufficiency is required. The national UAV development and procurement framework approved in October 2025 recognizes the need for additional demand and international cooperation in two of its four pillars: expanding domestic and international demand, and fostering technological advancement and international cooperation.⁹ In discussions with stakeholders and researchers during the Taiwan-US-

Europe Policy Program (TUPP) in March 2026, the necessity of scaling domestic Taiwanese production through exports was repeatedly emphasized. European nations were mentioned as potential buyers.

In the EU, drone production capacity lags even domestic demand. In 2024, only an estimated 8,000 units were produced, and even by early 2026 the bloc's industrial base could cover less than 30% of member-state demand.¹⁰ Taiwanese stakeholders have aptly identified the European market as a major export destination, and Europe indeed emerged in 2025 as a prime destination with more than 65,000 units imported from Taiwan. Driven by Chinese export restrictions, imports from Taiwan have continued to grow rapidly in 2026: More than 80,000 complete drones were imported in just two months.¹¹ In January 2026 the European Parliament adopted a resolution on drones and new systems of warfare, specifically recommending Taiwan as a partner for enhanced cooperation in drone technologies.¹² In fact, joint ventures and plans for production sites by Taiwanese companies in Poland, Czechia, and the Baltic states already benefit the EU in its ambition to onshore drone production.¹³

While this may benefit Taiwan in expanding supply chains, such facilities could hardly supply the island's armed forces if a contingency were to arise. Three additional caveats must be considered: First, the bulk of current drone exports to Europe are ultimately routed to Ukraine, and the export volume thus depends on wartime demand. Second, even though EU member states cannot cover their own drone demand, dependence on production facilities in Taiwan would likewise present a critical vulnerability during a crisis in the Strait, one that may be accompanied by Russian aggression against an EU member state. Third, the lack of formal recognition of Taiwan by member states constrains potential cooperation models, specifically more

formal government-to-government schemes. This means further cooperation needs to ensure resilient production capacity in both the EU and Taiwan, recognize the development of knowledge and scalability through latent industrial capacity, and navigate the complexities of member states' lacking recognition of Taiwan. In fact, the biggest challenges, but also the biggest prospects for cooperation, are upstream of drone assembly, particularly in critical dependencies in the supply chain itself.

The Real Challenge: Upstream Dependency

The assembly of complete UAVs (that can be modified with different payloads as Ukraine is doing) represents the drone supply chain problem only at the surface. China still retains dominant control of the supply chain, for components and for refining rare earths. While Taiwan has considerable capacity in UAV battery module production, with one supplier alone exporting 20,000 battery modules per month to Ukraine, the upstream supply chain leads to China.¹⁴ About 90% of sintered rare-earth permanent magnets needed for drone motors are produced in China, which also processes 70% of graphite and two-thirds of lithium needed for batteries.¹⁵ By 2025, if not earlier, China was using its controlling position to exert pressure with increasingly strict export controls. European countries have not been completely cut off from Chinese-made components, but Beijing has heightened scrutiny of exports of motors, batteries, flight controllers, optical sensors and other components. Further, even as Beijing continues to supply Russia, it bans the export of these components if authorities suspect their transfer to Ukraine or military use in general.¹⁶

As a 2025 report by the Research Institute for Democracy, Society and Emerging Technologies outlines, the Taiwanese industry continues to struggle with reliance on foreign technologies and supply-chain bottlenecks despite its better position in the electronics and semiconductor supply chain, including in battery assembly.¹⁷ This mirrors the dependencies and localization efforts with which Ukraine struggles, not least due to Chinese export restrictions. By the end of 2025, Ukrainian UAV manufacturing still relied on Chinese supplies for 60% to 80% of components while localization efforts had reached only 40% for bodies and batteries, and just 15%–20% for other complex inputs.¹⁸

These dependencies directly tie into EU efforts to de-risk its own dependencies and the realization that earlier initiatives such as the European Raw Materials Alliance (ERMA) were insufficient to address the challenge. The Critical Raw Materials Act (CRMA) of 2024 and the RESourceEU Action Plan of 2025 provide more robust frameworks. Through the latter, the EU specifically recognizes the importance of mining and processing for the resilience of defense industrial supply chains. This de-risking framework also recognizes the need for like-minded partners through establishing Strategic Partnerships, primarily when it comes to mining but also in downstream parts of the supply chain.¹⁹ By early 2026, the EU had signed 14 Strategic Partnerships with third countries, with projects focusing on mining and creating local processing capacities.²⁰ As a recipient rather than a supplier, Taiwan would, of course, present an unlikely candidate for such a Strategic Partnership. Considering the convergence of interests and a strong downstream position, implicit cooperation in this area should nonetheless be pursued.

Policy Recommendations: Alignment Instead of Formality

The EU-Taiwan Trade and Investment Dialogue already presents a coordination forum under which working groups and technical exchanges are organized. Going forward, an additional bilateral working group focusing on the drone supply chain and technical exchanges on respective aspects of semiconductors, battery technology and other drone components, and mineral supply chains should be established. It is crucial that the consultation not be limited to UAVs but also anticipate future demand and requirements related to UGVs, USVs, and UUVs. Even though political constraints widely block formal frameworks of cooperation, closer alignment—through Taiwanese investments in CRMA Strategic Projects, for example—can be coordinated through the EU-Taiwan Trade and Investment Dialogue. This more holistic approach of cooperation and coordination on all aspects of the supply chain forestalls the perils of silo thinking, which solely focuses on drones and components produced or exported. These formats could also be used for matchmaking and promote business-to-business relationships that benefit the public goals of both sides.

As others have outlined in detail before, civilian industries such as automotive manufacturing could be quickly retooled to provide scalability in the event of armed conflict²¹—but only if supply chains are in place that cannot be cut off by China. The key to expanding drone industrial bases in the EU and Taiwan thus lies in securing upstream inputs and setting the conditions for scalability during a crisis. In light of China's advantageous position, pooling resources is the sensible way forward due to the like-minded nature of both partners and the compatible strengths of established knowledge bases and capacity to mobilize capital. Both sides should also stockpile inputs and components for drones before a crisis to increase

resilience against supply chain shocks. Stockpiling can be applied for some complete drone types that allow payload modularization and adaptability for the demands of electromagnetic warfare, and, more importantly, for components, where applicable. The creation of stockpiles can also be leveraged to expand supply chain capacity in peacetime.

China's inevitable retribution may deter European capitals, not least in light of Lithuania's experience after 2021, when Beijing employed coercive economic measures against the country in response to its decision to allow Taiwan to open a representative office in Vilnius under the name "Taiwanese Representative Office" rather than "Taipei". Beijing viewed this as a major violation of its "One China" principle. However, the geopolitical shifts since then demonstrate why European policymakers should pursue deeper cooperation even if it risks Chinese ire. China continues to support Russia in its war of aggression against Ukraine, the core European security interest, while increasingly restricting exports to Ukraine and Europe as a whole. Europeans have lagged in imposing costs on China for this policy. The relationship with Taiwan is, of course, not a tool to punish Beijing. However, deepening ties would strengthen cooperation with a like-minded partner and project a more confident and strategically self-assured EU. If the bloc seeks to translate its ambitions for strategic autonomy into geopolitical practice, deeper engagement with Taiwan becomes a logical step.

Endnotes

¹ Hong-Lun Tiunn, "US-Taiwan Defense Partnership 2.0: Taiwan's UAV Doctrine and Industrial Base", *The Diplomat*, April 4, 2025. <https://thediplomat.com/2025/04/us-taiwan-defense-partnership-2-0-taiwans-uav-doctrine-and-industrial-base/>

² Krzysztof Niecypor and Sławomir Matuszak, "Game of drones: The production and use of Ukrainian battlefield unmanned aerial vehicles", *Centre for Eastern Studies (OSW)*, October 14, 2025. <https://www.osw.waw.pl/en/publikacje/osw-commentary/2025-10-14/game-drones-production-and-use-ukrainian-battlefield-unmanned>

³ Jorge Rivero, "Networked for War: Lessons from Ukraine's Ground Robots", *Modern War Institute*, March 10, 2026. <https://mwi.westpoint.edu/networked-for-war-lessons-from-ukraines-ground-robots/>

⁴ *Business Insider*, "Ukraine Is Betting Big on War Robots, with Plans to Buy 25,000 and Remove Humans from Front-Line Supply Runs", April 2026. <https://www.businessinsider.com/ukraine-ground-robots-troops-uncrewed-ground-vehicles-first-quarter-2026-4>

⁵ Ministry of Defence of Ukraine, "A sinking fleet: Russia's largest losses in the Black Sea and the Sea of Azov during the war", April 17, 2026. <https://mod.gov.ua/en/news/a-sinking-fleet-russia-s-largest-losses-in-the-black-sea-and-the-sea-of-azov-during-the-war>

⁶ Samara Duerr, "Drone Superpower: Ukraine's UAV Success and Where Taiwan-Ukraine Cooperation Fits In", *Research Institute for Democracy, Society and Emerging Technology*, April 22, 2026, p. 12. <https://dset.tw/en/research/000491-2/>

⁷ Jules Quartly, "Taiwan's China-Free Drones Flying Off the Shelves", *Taiwan News*, March 14, 2026. <https://www.taiwannews.com.tw/news/6320710>

⁸ Leticia Batista Cabanas and Elisabeth Heinz, "Mass Drone Warfare Is Europe's Rising Security Threat", *Euronews*, April 14, 2026. <https://www.euronews.com/my-europe/2026/04/14/mass-drone-warfare-is-europes-rising-security-threat>

⁹ Ministry of Economic Affairs, Republic of China Executive Yuan, "Developing the drone industry", October 29, 2025. <https://english.ey.gov.tw/News3/9E5540D592A5FECDD07bcbd8d-3929-416e-8bfd-c2f17847cad5>

¹⁰ Cabanas and Heinz, "Mass Drone Warfare Is Europe's Rising Security Threat".

¹¹ Duerr, "Drone Superpower".

¹² European Parliament, "Drones and New Systems of Warfare – the EU's Need to Adapt to Be Fit for Today's Security Challenges" [Resolutions], January 22, 2026. https://www.europarl.europa.eu/doceo/document/TA-10-2026-0020_EN.html

¹³ Duerr, "Drone Superpower".

¹⁴ Hong-Lun Tiunn, Cathy Fang, Chun-Kuei Lai, Jenny Li, and Elizabeth Ru-Tung Sun, "Drones for Democracy: U.S.-Taiwan Cooperation in Building a Resilient and China-Free UAV Supply Chain", *Research Institute for Democracy, Society and Emerging Technology*, June 2025, p. 60. <https://dset.tw/en/research/drones-for-democracy-the-strategic-imperative-for-u-s-taiwan-uav-cooperation/>; Duerr, "Drone Superpower", p. 92.

¹⁵ Macdonald Amoah, Morgan Bazilian, Jahara Matisek, and Katrina Schweiker, "The Drone Supply Chain War: Identifying the Chokepoints to Making a Drone", *Center for Strategic and International Studies*, December 9, 2025. <https://www.csis.org/analysis/drone-supply-chain-war-identifying-chokepoints-making-drone>

¹⁶ Charles Clover, William Langley, and Chris Cook, "Russia, Ukraine and the Race for Chinese Drone Components", *Financial Times*, January 21, 2026. <https://www.ft.com/content/58416bf8-97d0-4d99-8152-cff9ec2dd3ef>

¹⁷ Tiunn, et al., "Drones for Democracy".

¹⁸ UA News, "Ukraine Localises Production of Drone Components", December 3, 2025. <https://ua.news/en/war-vs-rf/ukrayina-lokalizuije-virobnitstvo-komponentiv-dlia-droniv>

¹⁹ European Commission, "RESourceEU Action Plan", December 3, 2025. https://single-market-economy.ec.europa.eu/document/download/01c448d6-dc93-40d7-9afe-4c2af448d00c_en

²⁰ European Commission, "Commission Selects 13 Strategic Projects in third countries to secure access to raw materials and to support local value creation" (Press release), June 4, 2025. https://ec.europa.eu/commission/presscorner/detail/en/ip_25_1419

²¹ Martin C. Feldmann and Gene R. Keselman, "Factories First: Winning the Drone War Before It Starts", *War on the Rocks* (Cogs of War), July 17, 2025. <https://warontherocks.com/2025/07/factories-first-winning-the-drone-war-before-it-starts/>; Chad P. Wanek, "Arsenal in Transition: Lessons from World War II Industrial Conversion", *Center for Strategic and Budgetary Assessments*, 2026. <https://csbaonline.org/resource/arsenal-in-transition-lessons-from-world-war-ii-industrial-conversion/>

Creative Workarounds

Taiwan's Informal Defense Partnerships in a Shifting Indo-Pacific Region

By Rachel Vandenbrink

"The most important thing is to embed Taiwan more fully into Indo-Pacific security frameworks", Taiwan's foreign minister, Lin Chia-lung, said in a media interview this year.¹ The remark was striking coming from a government that lacks formal standing in any regional security mechanisms and has long anchored its security almost exclusively in its bilateral relationship with the United States. As the regional security architecture has shifted toward networked and integrated defense relationships, however, the imperative for Taiwan to expand beyond the US-Taiwan bilateral relationship has grown sharper. In response, Taiwan has quietly been building defense partnerships through informal and creative mechanisms, cultivating new forms of maritime and coast guard cooperation, parliamentary exchanges, "Track 1.5" strategic dialogues, defense industrial base collaboration, and training exchanges. Lin's comment reflects a strategic reprioritization that Taiwan has already set in motion: cultivating deeper defense relationships with a more diverse set of partners.

Achieving this aim remains a tall order, especially for a government shut out of the formal cooperation mechanisms that most countries take for granted. The institutions responsible for Taiwan's defense diplomacy are being asked to do more—and do it through bespoke methods—at a time when their capacity is already heavily committed. Taiwan's defense and national security apparatus must simultaneously strengthen the island's defenses, support a sweeping civil defense effort, continue to enhance training with the United States, and manage a surge of interest from international partners seeking

to learn from Taiwan's experience with whole-of-society resilience. Expanding defense cooperation with limited institutional bandwidth requires a careful and multifaceted strategy: prioritizing partnerships with the greatest operational coordination value, pursuing second-tier relationships on lower-sensitivity topics, institutionalizing existing frameworks so that progress is insulated from shifts in political headwinds, and managing the information security risks that could undermine it all. The more Taiwan can deepen its defense relationships with critical partners, the more it can demonstrate to Beijing that regional security cooperation is not just rhetorical, but operational, coordinated, and real.

Strategic Context

Taiwan's push to expand its defense partnerships has come against a backdrop of significant shifts in the regional security architecture. During the early 2020s, spurred by US efforts for "integrated deterrence" and "networked deterrence", regional countries moved toward establishing minilaterals like AUKUS, the Quad, and trilateral US-Japan-Philippines cooperation. These frameworks reflected a shared recognition that deterring China required not just American power but a networked architecture of capable, coordinated allies and partners.² Formally, Taiwan sat outside these frameworks, but it was very much their animating concern.

The regional security landscape has grown more complicated since then. Friction over trade has strained some alliance relationships, and confidence in the reliability of American strategic commitments has fallen, prompting some partners to diversify their relationships to hedge against uncertainty about US staying power.³ Yet the underlying threat perceptions that drove the move toward networked deterrence have not changed—if anything, they have sharpened—and regional powers have continued to build up their own independent and collective military capabilities, often under the banner of greater burden-sharing. The result is a regional security architecture that places the island at the center of a set of overlapping security relationships that Taiwan has a profound interest in shaping.

Within this context, Taiwan's cooperation options are constrained because it lacks formal, treaty-based defense relations with any partner, even the United States. Unlike most regional countries, Taiwan does not engage in regular ministerial-level defense exchanges with its counterparts, it is shut out of regional defense forums, and its armed forces do not participate in multinational exercises such as RIMPAC or Cobra Gold. Taiwan maintains military attaché offices or coordination groups in only 25 countries.⁴ All of this means Taiwan is heavily reliant on working through the United States for security cooperation and training.

Taiwan's Ambitions for Expanded Partnerships

Recognizing the imperative to expand its security connections beyond the United States, Taiwan has quietly pursued creative ways to deepen defense cooperation with new partners, focused not just on informational exchange but increasingly on improving

combat readiness and operational coordination. In a rare interview on the topic, Minister of National Defense Wellington Koo told reporters in late 2024 that Taiwan had strengthened its partnerships with "the United States and other friends and allies" to deepen military cooperation that "contributed to the improvement of the national military's combat effectiveness". He emphasized that Taiwan did not publicize such cooperation to respect friends and allies and avoid "unnecessary interference".⁵

Taiwan has enshrined this ambition in its latest strategy documents. The 2025 Quadrennial Defense Review highlighted "Expanding Security Partnerships with International Partners" as a priority area and pledged that Taiwan "will make the most of favorable atmosphere in international democratic communities to collaborate with like-minded countries to form a multilateral security network".⁶ It further stated that the Ministry of National Defense (MND) would expand international exchanges on intelligence-sharing, scientific R&D, cybersecurity, anti-gray zone activities, and cognitive warfare threats "with the goal of establishing a regional defense mechanism", and work through the MND's Institute for National Defense and Security Research to conduct Track 2 engagements.⁷ The 2025 National Defense Report similarly highlighted how partner countries increasingly attach importance to Taiwan's armed forces' operational capabilities, and pointed to informal exchanges on cybersecurity and military medicine as "alternative" means to building closer bilateral relations "when actual visits cannot be made".⁸ Taken together, these documents signal that expanding defense partnerships is no longer a diplomatic aspiration but an operational priority embedded in Taiwan's defense planning.

Informal Mechanisms and Their Limits

Under this policy guidance, Taiwan has pursued a number of cooperation initiatives—multilaterally with global partners and bilaterally with key regional ones—that are beginning to bear fruit.

Key among them is Taiwan's participation in the Global Cooperation and Training Framework (GCTF), established in 2015 as a vehicle for multilateral capacity-building and administered by the American Institute in Taiwan with participation from Australia, Canada, Japan, and the United Kingdom. Over the past decade the GCTF has hosted nearly 100 international workshops, drawing more than 10,900 participants from over 130 countries, on topics including cybersecurity, supply chain resilience, humanitarian assistance, and countering disinformation.⁹ With its topics deliberately kept at the softer end of the security spectrum, the framework is a vehicle for sharing best practices and building working relationships, not for operational coordination or contingency planning. But within those limits it has become Taiwan's most valuable multilateral channel: one of the few venues where Taiwan can participate as an equal contributor and capacity-builder rather than a diplomatic outlier, and a proven platform for drawing in a wide range of partners on security topics.

Beyond the GCTF's multilateral framework, Taiwan has pursued deeper bilateral cooperation with its most strategically important neighbors including Japan, the Philippines, and Australia. Taiwan has used maritime cooperation, parliamentary and political dialogue, and Track 1.5 strategic engagement with these countries to, in particular, lay a foundation for stronger options for operational coordination.

With Japan, in the absence of formal government-to-government defense channels, Taiwan has turned

to two creative alternatives, coast guard cooperation and parliamentary dialogue, to lay the groundwork for a deeper security relationship. Regarding the former, the Japanese and Taiwanese coast guards conducted maritime search and rescue drills for the first time in 2024 and 2025, a notable milestone given long-standing sovereignty disputes that had complicated bilateral cooperation for decades.¹⁰ The drills, which Japan classifies as “exchanges” rather than exercises, built on years of practical maritime collaboration, including a 2017 memorandum of understanding on search and rescue signed by their respective liaison offices.¹¹ Concerning parliamentary dialogue, Japan's Liberal Democratic Party in 2021 formed a Taiwan project team and launched security talks with Taiwan's Democratic Progressive Party that were structured as a ruling-party equivalent of a two-plus-two security dialogue.¹² These dialogues have continued in subsequent years, covering topics including countering Chinese influence operations and intelligence sharing. Since these informal initiatives began, Japan has articulated a closer connection between Taiwan's security and its own. In November 2025, Japanese Prime Minister Sanae Takaichi said that a Taiwan contingency could constitute a “survival-threatening situation” for her country, potentially bringing such a scenario within Japan's legal framework for collective self-defense.¹³

With the Philippines, Taiwan has used maritime cooperation as a creative mechanism to build an increasingly substantive security relationship rooted in shared strategic geography. The Bashi Channel separates northern Luzon from Taiwan's southern coast by only about 190 nautical miles, making any Taiwan contingency an acute Philippine concern, and coast guard cooperation has been the natural entry point.¹⁴ Taiwan has trained Philippine coast guard officers since 2021,¹⁵ and last year the two coast guards conducted joint patrols in the Bashi Channel.¹⁶ Taiwan also reportedly sent observers to US-Japan-

Philippines exercises in the Philippines' Batanes islands in 2025.

The Ferdinand Marcos administration in Manila has been notably permissive toward Taipei, easing restrictions on Philippine officials visiting Taiwan. President Marcos stated this year that his country would likely be involved in any conflict over Taiwan due to the Philippines' proximity to the island,¹⁷ and Defense Secretary Gilberto Teodoro told reporters that Manila is working more closely with Taiwan and other regional partners to build an "active defense alliance".¹⁸ Their comments reflect real gains for Taiwan, but a successor government could revert to greater caution, making it urgent to convert the present informal ties into standing mechanisms.

With Australia, a promising avenue has been Track 1.5 engagement. Canberra's policy community is increasingly debating how far to go in engaging Taiwan through Track 1.5 and Track 2 dialogues, a conversation that has gained momentum in recent years. The participation of former Prime Minister Scott Morrison in the 2025 Taipei Security Dialogue, for example, is a visible marker of Australia's growing interest in exploring more engagement with Taiwan.¹⁹ Such exchanges involving former senior officials and academics can carry weight by signalling political backing and building personal relationships that formal cooperation will eventually depend on. The challenge is that Track 1.5 channels can lay groundwork but cannot substitute for institutional momentum.

These informal mechanisms have achieved tangible gains, but they share a key weakness. They rely on political goodwill, personal relationships, and favorable windows that can close. Ad hoc interactions lack the institutionalized rhythm that a calendar of regular two-plus-twos and chiefs of defense meetings provides to build momentum, drive deliverables, and ensure sustained progress over time. Without

stronger institutional foundations, Taiwan's defense partnerships remain vulnerable to changes in political leadership. But that weakness should not obscure what these mechanisms have achieved or what remains possible within their constraints. Maritime cooperation, parliamentary dialogues, Track 1.5 and academic exchanges, and multilateral capacity-building are durable tools that can be deepened and used deliberately to advance Taiwan's security partnerships even in the absence of formal alliances or relations.

A Strategy for Expanding Partnerships

Taiwan's informal defense diplomacy has generated momentum but also placed demands on a government already stretched by an ambitious agenda of military reform, enhanced training with the United States, and a sweeping whole-of-society resilience effort. Adding to that pressure is a surge of interest from European partners, drawn by Taiwan's experience with drone technology and civil society resilience to disinformation efforts, as well as interest in comparing lessons learned from the war in Ukraine. With finite capacity and competing priorities, Taiwan cannot pursue every opportunity equally. An efficient, selective strategy is essential. The following recommendations are intended to aid in developing such a strategy.

- Prioritize and institutionalize cooperation efforts with Japan, Philippines, Australia.** The first priority is deepening and institutionalizing cooperation with the partners that could bring the greatest operational coordination value for a Taiwan contingency. Japan should be at the top of that list of partners: geographic proximity

creates similar contingency concerns, threat perceptions are closely aligned, and Taiwan's most advanced existing defense relationship, barring that with the United States, is with Tokyo. The Philippines, however, represents the most politically open window for visible cooperation right now—a window that could close if political administrations change—with significant room to expand operational coordination beyond coast guards. Australia, where new conversations about engaging Taiwan are emerging, offers a natural avenue for deeper coordination as a member of the Five Eyes intelligence-sharing alliance with the United States. But deepening these relationships is not enough. Taiwan must also work to institutionalize them, converting informal practices into standing mechanisms such as regularized schedules for coast guard joint exercises, formalized working groups among defense research institutions, and memoranda of understanding that create bureaucratic constituencies for continued engagement on both sides, insulating progress from changes in political leadership.

- **Use multilateral channels to expand reach while addressing lower-sensitivity topics.** European and other partners are increasingly interested in Taiwan's experience with drone technology, gray-zone coercion, countering mis- and disinformation, and whole-of-society resilience. Engagement on these topics is an important complement to the bilateral relationships that matter most in a crisis and remains key to building broad awareness and sympathy across a wide coalition. Given Taiwan's need to prioritize ruthlessly, multilateral formats like the GCTF can offer an efficient vehicle for Taiwan to

use low-sensitivity cooperation to reach many partners simultaneously.

- **Manage information security.** Without a Five Eyes framework (which establishes common classification standards and trusted channels for handling sensitive material), sharing sensitive information is difficult. China's intelligence penetration in Taiwan runs deep, extending to members of the government and military.²⁰ The more partners Taiwan brings into sensitive discussions, the more important information security becomes. Any expansion of defense cooperation must be accompanied by serious investment in information security protocols—not just to protect Taiwan's own secrets but to give partners the confidence needed to share sensitive material with Taipei.

To be sure, there is a limit to how far other countries will go to support Taiwan in a conflict with China, and strengthened defense partnerships are not a cure-all for Taiwan's defense needs.²¹ No matter how institutionalized these relationships become, they do not substitute for Taiwan's own military readiness or the credibility of US support. But in a cross-Strait contingency, Taiwan will not be counting on the United States alone; it will also be looking to regional and global partners for support that could shape the scope and success of any effort to defend the island. It only makes sense that Taiwan and those partners should have established ways of coordinating and building trust well before a crisis arrives.

Endnotes

¹ Gabriel Dominguez, "Taiwan's FM calls for Taipei to be part of 'first island chain' security framework", Japan Times, March 4, 2026. <https://www.japantimes.co.jp/news/2026/03/04/asia-pacific/politics/taiwan-foreign-minister-lin-chia-lung-interview/>

² Becca Wasser, "Networked deterrence in a multipolar Indo-Pacific", United States Studies Centre, February 29, 2024. <https://www.usssc.edu.au/networked-deterrence-in-a-multipolar-indo-pacific>

³ Luke Collin, "Correcting Course in the Indo-Pacific", War on the Rocks, April 30, 2026. <https://warontherocks.com/correcting-course-in-the-indo-pacific/>

⁴ National Defense Report Editorial Committee, "Republic of China National Defense Report 2025", Ministry of National Defense, October 2025. <https://www.mnd.gov.tw/newupload/ndr/114/114ndreng.pdf>

⁵ Ben Blanchard, "Taiwan deepening security cooperation with US, other 'allies'", Reuters, September 18, 2024. <https://www.reuters.com/world/taiwan-deepening-security-cooperation-with-us-other-allies-2024-09-19/>

⁶ Quadrennial Defense Review Editing Committee, "2025 Quadrennial Defense Review", Ministry of National Defense, March 2025, p. 61. <https://bit.ly/4hTAY42>

⁷ Ibid.

⁸ NDR Editorial Committee, "Republic of China National Defense Report 2025", p. 97.

⁹ American Institute in Taiwan, "Global Cooperation and Training Framework", <https://www.ait.org.tw/global-cooperation-and-training-framework-gctf/>

¹⁰ The Yomiuri Shimbun, "Japan, Taiwan To Conduct Regular Joint Maritime Drills, with Other Partners Possibly Joining in the Future", October 3, 2025. <https://japannews.yomiuri.co.jp/politics/defense-security/20251003-284457/>

¹¹ Ibid.

¹² Michael Mazza, "Party-to-Party Dialogue between Taiwan and Japan Points the Way to Closer Security Ties", Global Taiwan Institute, August 25, 2021. <https://globaltaiwan.org/2021/08/party-to-party-dialogue-between-taiwan-and-japan-points-the-way-to-closer-security-ties/>

¹³ Mari Yamaguchi and Ken Moritsugu, "Japan and China exchange barbs after PM Takaichi's remarks over Taiwan", Associated Press, November 15, 2025. <https://apnews.com/article/japan-china-taiwan-emergency-takaichi-0cefc2b4e4f1cda16a4c8bfef033be2d>

¹⁴ Edcel John A. Ibarra, "Entangled Fronts: The Philippines' Anxiety over a Taiwan Crisis", National Bureau of Asian Research. <https://www.nbr.org/publication/entangled-fronts-the-philippines-anxiety-over-a-taiwan-crisis/>

¹⁵ Kelvin Chen, "Taiwan, Philippines plan to deepen coast guard cooperation", Taiwan News, May 14, 2024. <https://www.taiwannews.com.tw/news/5685819>

¹⁶ Rebecca Tan, Frances Mangosing, and Pei-Lin Wu, "The Philippines is quietly working with Taiwan to counter China", The Washington Post, July 14, 2025. <https://www.washingtonpost.com/world/2025/07/14/philippines-taiwan-security-ties-china/>

¹⁷ Cliff Harvey Venzon, "Marcos Says Philippines Would Be Involved in Any Taiwan Conflict", Bloomberg News, May 19, 2026. <https://www.bloomberg.com/news/articles/2026-05-19/marcos-says-philippines-would-be-involved-in-any-taiwan-conflict>

¹⁸ Andreo Calenzo, Haslinda Amin, and Philip Heijmans, "Philippines Seeks Closer Ties With Taiwan, Adversaries of China", Bloomberg News, May 30, 2026. <https://www.bloomberg.com/news/articles/2026-05-30/philippines-seeks-closer-ties-with-taiwan-adversaries-of-china>

¹⁹ Office of the President, Republic of China, "President Lai Meets 2025 Taipei Security Dialogue Participants", October 9, 2025. <https://english.president.gov.tw/News/7020>

²⁰ Joyu Wang, "The Chinese Spy Machine Infiltrating Taiwan's Military", The Wall Street Journal, January 21, 2026. <https://www.wsj.com/world/asia/taiwan-military-china-spy-network-a56ec8da?eafs>

²¹ Lyle Goldstein, "Target Taiwan: Limits of Allied Support", Defense Priorities, October 15, 2025. <https://www.defensepriorities.org/explainers/target-taiwan-limits-of-allied-support/>

The KMT, the CCP and Party-to-Party Dialogue

By Thomas Yoshimura

On April 10, 2026, Cheng Li-wun became the first sitting chair of the Kuomintang (KMT) since 2016 to meet with Xi Jinping, secretary general of the Chinese Communist Party (CCP). For the KMT chair, the summit at the Great Hall of the People marked the culmination of a multi-day visit to the People's Republic of China (PRC), widely framed as a "peace trip" and closely followed by international media and analysts.

International commentary largely portrayed the visit as a successful effort by Xi Jinping to weaken the Democratic Progressive Party (DPP) administration of Lai Ching-te. Critics, however, interpreted the meeting as further evidence that the KMT chair overestimated both the prospects for dialogue with Beijing and her own leverage over the PRC. Less prominent analyses instead emphasized the domestic political dimension of the visit, linking Cheng's apparent display of strength to the upcoming local elections in the fall and the emerging contest over the KMT's presidential ticket for 2028.

A closer examination of Taiwan's current party landscape, however, points to a broader process of internal struggle and attempted rejuvenation within the KMT after years out of power. The episode therefore underscores the importance of paying closer attention to the KMT's internal evolution as a key variable in both Taiwanese politics and cross-Strait relations. At the same time, the party-to-party framework chosen by the KMT and CCP provides a concrete example of how similar channels of

engagement might be explored by interested actors in Europe.

The PRC's Perspective

Arguably, the easiest and most common way to interpret the meeting between Xi Jinping and Cheng Li-wun is through a PRC-centered perspective.¹ Beijing, and especially the CCP, regards Taiwan as an inseparable part of a single nation. According to Beijing's "One China Principle", there is only one China in the world, Taiwan is an inalienable part of China, and Beijing is the sole legitimate government representing all of China, following the Communist victory over the Nationalists and the creation of Republic of China in the Chinese Civil War. Consequently, the idea of a sovereign Taiwanese nation-state is unacceptable to the CCP, which neither recognizes nor accepts a separate government in Taipei. The Democratic Progressive Party (DPP) and leading figures such as former President Tsai Ing-wen and Lai Ching-te are perceived by the CCP as supporting Taiwan's independence and thus are targets of continuous political pressure and propaganda campaigns.

Although the KMT was the CCP's principal enemy during the civil war, it has since become Beijing's preferred interlocutor and the most acceptable alternative to the DPP in managing cross-Strait affairs. Relations with Beijing have arguably remained Taiwan's central strategic issue for decades and continue to be among the most significant items on

the island's political agenda. Conventional wisdom portrays the KMT as a party that emphasizes Chinese cultural heritage and identity while maintaining a longstanding belief in dialogue and the possibility of peaceful coexistence with the PRC.² As a result, aiming for greater openness among the people of Taiwan toward Beijing and the promotion of cross-Strait dialogue are often equated with strengthening the KMT itself.

By suspending official communication channels with the DPP while simultaneously granting public and high-profile access to the incumbent KMT chair, Beijing seeks to delegitimize the DPP in the eyes of both Taiwanese society and the wider international community. At the same time, by shining a spotlight on divergent positions on emotionally charged issues such as cross-Strait relations, media coverage and public debate around the occasion becomes a tool for Beijing to further deepen polarization within Taiwan's domestic politics. International attention surrounding the visit also enabled the CCP to reinforce familiar narratives portraying Beijing as open to dialogue and committed to peace.

However, the promises made by the CCP regarding improved cross-Strait relations, in statements during the Xi-Cheng meeting and released afterward, remained conditional on acceptance of the 1992 Consensus: In 1992, the PRC and Taiwan, under a KMT administration, declared an agreement "that the two sides of the Strait are part of 'one China' even though they disagree over who has sovereignty and don't recognize each other's legitimacy".³ The KMT usually adds a set phrase noting that there are respective interpretations of the term "one China", but the PRC consistently omits this. The CCP's post-meeting statements also spoke strongly in opposition to Taiwanese independence and so-called foreign interference.⁴ Cheng Li-wun later also directly linked a

KMT victory in 2028 to the possibility of a return visit by Xi Jinping.⁵

Cheng Li-wun Thought

At the same time, Cheng Li-wun's own motivations may differ somewhat from those of the CCP leadership. She appears genuinely convinced of her ability to manage relations with both Xi Jinping and the PRC. Her political ambitions seem rooted in reversing the current trajectory of escalation in cross-Strait relations and restoring a version of the comparatively stable environment associated with the presidency of Ma Ying-jeou. Before and after her visit to Beijing, and again in the days preceding the summit meeting between US President Donald Trump and Xi Jinping, Cheng repeatedly articulated a vision of Taiwan pursuing a more autonomous diplomatic posture and, at times, even serving as a mediator between the PRC and the United States.⁶

She presents this approach as a sincere effort to recalibrate Taiwan's relations with both Beijing and Washington in order to reduce tensions, avoid military conflict, and ultimately preserve peace. From Cheng's perspective, Taiwan should not be forced to choose between the two powers but instead cultivate its own strategic balance and room for maneuver. Cheng has argued that peace can best be preserved through a combination of credible deterrence, restraint on moves toward formal independence, and the maintenance of open channels of dialogue with Beijing. Within this framework, the KMT's role is to facilitate cross-Strait communication while simultaneously maintaining strong ties with Washington. The announcement of a planned visit to the United States in June following her April trip to the PRC suggests that at least some aspects of

her political actions are consistent with this broader strategic vision.⁷

Yet an exclusively international perspective can only partially explain the broader significance of Cheng Li-wun's visit. A more complete understanding requires situating the visit within the context of Taiwan's domestic politics and the KMT's internal dynamics.

A New Formula

First, Cheng's messaging appeared to contain subtle yet potentially significant departures from traditional KMT formulations. During the meeting in Beijing, both Xi and Cheng repeatedly referred to the 1992 Consensus, yet Cheng did not add the formula of "different interpretations", but joined Xi in explicitly rejecting Taiwanese independence. At the same time, both leaders stressed the rejuvenation of the Chinese nation and the importance of strengthening ties between people on both sides of the Taiwan Strait. Notably, however, Xi refrained from explicitly discussing unification, invoking the PRC's "One China Principle", or using the phrase "One Country, Two Systems". Xi Jinping also consistently referred to "China" rather than "the PRC". Taken together, these rhetorical choices suggest that while Cheng again demonstrated considerable alignment with Xi, she may also have exercised at least limited influence over the wording and framing adopted at the highest political level.⁸

Second, Cheng's speech at the Sun Yat-sen Mausoleum in Nanjing—an earlier stop on the trip that attracted far less international attention—may provide additional insight into her political motivations. Although she made repeated references to the Chinese people on both sides of the Taiwan

Strait and invoked Japan and Japanese militarism in the early 20th century in language that some observers regarded as echoing CCP rhetoric, analysts also noted an apparent attempt to connect the legacy of Sun Yat-sen more directly to a specifically Taiwanese perspective. In doing so, she appeared to move beyond the more traditional Chinese nationalist framing associated with figures such as Ma Ying-jeou. Whether successful or not, this may reflect an attempt to "Taiwanize" the KMT and reposition the party closer to mainstream public opinion in Taiwan ahead of the elections scheduled for November 2026 and 2028.⁹

It's the Elections, Stupid

The KMT lost the presidency in 2016, and currently its ability to block elements of DPP policy in parliament is enabled only through a majority in cooperation with the Taiwan People's Party (TPP). The two parties agreed to field joint candidates in the November elections in order to maximize the electoral potential of their political camp. The KMT needs a strong performance this year to set the stage for its presidential bid, both in absolute terms and relative to the strong performance in the last local elections, held in 2022. More than upholding the already high number of constituencies that elected KMT candidates before, winning in specific, symbolic cases (like the city of Kaohsiung, a traditional DPP stronghold) is considered of particular importance. Ultimately, however, the party's primary objective is victory in the 2028 presidential election and a return to power in Taipei. The November elections are widely regarded as a critical milestone on the path toward that broader goal.

For Cheng Li-wun, this creates a powerful political incentive. She secured the KMT chairmanship last

year by only a narrow margin, and her election was accompanied by criticism stemming from allegations of illicit support and unusually open expressions of approval from the PRC. Moreover, holding the position of party chair does not automatically translate into full control over the KMT's broader political direction. Internal divisions became particularly visible during debates over the Special Defense Budget. Cheng appears to have used relations with Beijing—and especially the political opportunity provided by a high-profile visit—to consolidate her authority, boost her domestic political profile, and articulate a distinctive version of the KMT agenda on foreign policy and cross-Strait relations.¹⁰

If the KMT meets or even exceeds its own expectations in November, Cheng Li-wun would likely gain a stronger foundation from which to secure the party's nomination and begin building a campaign for 2028. Conversely, a poor electoral performance would almost certainly weaken her position, and tradition in Taiwan would oblige her to resign as party chair. Viewed from this perspective, Cheng's statements and actions during the PRC trip become less an expression of ideological orthodoxy and more part of an ongoing struggle for political power and influence within the KMT itself.

Inside the KMT

Regardless of whether Cheng Li-wun succeeds in reshaping the party's direction, the KMT may face deeper structural risks stemming from persistent internal divisions and the possibility of future electoral defeat. Rather than attempting to suppress intraparty opposition, a more sustainable strategy may lie in reconciling competing factions and combining their respective strengths in order to present a broader, more credible, and more responsible political

alternative. More than merely reviving earlier formulas—even in modified form—the KMT faces the challenge of generating entirely new momentum.

Traditional appeals to Chinese cultural heritage increasingly appear outdated and insufficiently responsive to changing identities and broader social developments in Taiwan. In particular, a cross-Strait policy centered primarily on opposing further movement toward independence or preserving an ambiguously defined status quo risks lacking the political dynamism necessary for an opposition party seeking to regain power. Such an approach may reinforce perceptions of ideological stagnation, a liability that could become especially damaging for a party attempting to reconnect with younger and more socially diverse segments of the electorate.¹¹

International understanding of these internal dynamics within the KMT remains relatively limited. Foreign interlocutors frequently focus their attention on government officials or the ruling party, while the KMT often appears underrepresented and less internationally visible than its DPP counterparts.

KMT International Affairs

Representatives of the KMT International Affairs Department privately describe their organization as a “shadow” version of Taiwan's Ministry of Foreign Affairs, complementing the work of the party's Mainland Affairs Department that functions in a similar way vis-à-vis the Mainland Affairs Council under the Executive Yuan. According to their description, the International Affairs Department concentrates primarily on engagement in Taipei with foreign diplomats, international media organizations, and visiting delegations.

The department itself reportedly consists of only a small number of permanent staff supported by a rotating group of volunteers. Approximately seven years ago, it was separated from the Overseas Affairs Department, which was responsible for relations with Taiwanese and Chinese communities abroad. In Washington, D.C., the KMT maintains only a small affiliated representative office. Overall, the share of party resources devoted to international affairs allows for only limited international outreach.

The KMT remains a member of the International Democratic Union (IDU), an international grouping of center-right political parties, and attempts to attend its annual summits. Semi-institutionalized party-to-party exchanges exist only intermittently with Japan's Liberal Democratic Party (LDP) and focus primarily on youth development, which has become a priority for the KMT leadership.

By contrast, the DPP has generally enjoyed a stronger position in communicating its perspective to international audiences. KMT representatives argue that their own political thinking is rooted in a more complex historical tradition that is often difficult to explain abroad. Consequently, they regard improving the party's international communication strategy as a major priority. Yet the KMT has lost much of its institutional expertise in foreign affairs to state institutions and continues to lack fully developed internal structures of its own. Building these much-needed capacities therefore remains an unfinished task.¹²

Lessons for Europe

The KMT's experience carries several implications for Europe. The KMT appears both interested in and in need of broader international networks beyond its

relationship with the CCP. More than the DPP, the KMT is struggling to redefine and communicate its core political message to a changing electorate rather than relying on an increasingly narrow traditional voter base. Understanding the debates taking place within the opposition has therefore become essential for understanding broader political and social developments in Taiwan itself.¹³

At present, however, the KMT appears heavily preoccupied with the restoration of political power, both for the party as an organization and for individual political figures pursuing, at times, highly controversial agendas that international observers often find difficult to interpret. Finally, the China factor remains significant in two distinct respects. On the one hand, the CCP appears to enjoy unusually direct access to the KMT, potentially granting Beijing privileged insights into the party as well as Taiwan's politics and, at least to some extent, political influence. Longstanding practices of highly accommodating treatment for KMT delegations visiting the PRC may also have reduced incentives for the party to cultivate alternative international partnerships. At the same time, however, the KMT is only one among many political parties worldwide—including in Europe—with which the CCP maintains institutionalized exchanges.

On the other hand, the CCP itself has effectively established party-to-party exchanges as politically acceptable within the framework of the PRC's "One China Principle". Engagement with political parties in Taiwan, including representatives of the KMT, should therefore also be regarded as compatible with respective European "One China" policies. It appears both reasonable and increasingly necessary that, alongside expanding political, parliamentary, and occasional governmental exchanges with Taiwan at multiple levels, political parties in Europe actively explore channels of dialogue with their Taiwanese counterparts—and vice versa.

Endnotes

¹ Chris Buckley and Amy Chang Chien, "Xi Invites Taiwan's Opposition Leader to Talk 'Peace' Ahead of Trump Summit", *The New York Times*, March 30, 2026. <https://www.nytimes.com/2026/03/30/world/asia/china-xi-taiwan-cheng.html>

² Phoebe Zhang, "No more 'cold peace' across Taiwan Strait", *South China Morning Post*, April 3, 2026. <https://www.scmp.com/news/china/politics/article/3348979/no-more-cold-peace-across-taiwan-strait-former-kmt-chairwoman-calls-rebuild-trust>

³ Bonnie Glaser, "Tsai Ing-wen and DPP Win Big in Taiwan", *CSIS*, January 18, 2016. <https://www.csis.org/analysis/tsai-ing-wen-and-dpp-win-big-taiwan>

⁴ Carol Yang, "Beijing pledges better Taiwan air and travel links after KMT leader's mainland China trip", *South China Morning Post*, April 12, 2026. <https://www.scmp.com/news/china/politics/article/3349782/beijing-pledges-better-taiwan-air-and-travel-links-after-kmt-leaders-mainland-china-trip>

⁵ *South China Morning Post*, "Cheng hopeful to invite Xi Jinping to Taiwan if the KMT wins 2028 election – as it happened", April 10, 2026. <https://www.scmp.com/news/china/politics/article/3349617/taiwans-opposition-leader-cheng-li-wun-speaks-after-historic-meeting-xi-jinping>

⁶ Laurence Chung, "Taiwan's Cheng Li-wun on cross-strait peace, meeting Xi Jinping and managing ties with the US", *South China Morning Post*, May 11, 2026. <https://www.scmp.com/news/china/politics/article/3353052/taiwans-cheng-li-wun-cross-strait-peace-meeting-xi-jinping-and-managing-ties-us>

⁷ Cheng Li-wun, "Taiwan Doesn't Have to Choose", *Foreign Affairs*, March 3, 2026. <https://www.foreignaffairs.com/taiwan/taiwan-doesnt-have-choose>

⁸ Brian Hioe, "The Domestic Politics of Cheng Li-wun's China Trip", *The Diplomat*, April 13, 2026. <https://thediplomat.com/2026/04/the-domestic-politics-of-cheng-li-wuns-china-trip/>

⁹ Han Yong Hong, "Cheng Li-wun and the 'Taiwanised' KMT", *Lianhe Zaobao/ThinkChina*, April 10, 2026. <https://www.thinkchina.sg/politics/cheng-li-wun-and-taiwanised-kmt-story-taiwan-may-not-buy>

¹⁰ Lyle Morris and Cheng Sheng-Wen, "Positioning the KMT in the U.S.-China-Taiwan Triangle", *Asia Society Policy Institute*, April 20, 2026. <https://asiasociety.org/policy-institute/positioning-kmt-us-china-taiwan-triangle-cheng-li-wuns-early-tenure>

¹¹ Dennis LC Weng, "The Kuomintang is Banking on Beijing", *East Asia Forum*, April 30, 2026. <https://eastasiaforum.org/2026/04/30/the-kuomintang-is-banking-on-beijing/>

¹² Danny Huang, interview by Thomas Yoshimura, May 7, 2026.

¹³ Lawrence Chung, "What's behind the KMT's internal splits over Taiwanese defence spending?", *South China Morning Post*, May 4, 2026. <https://www.scmp.com/news/china/politics/article/3352385/whats-behind-kmts-internal-splits-over-taiwanese-defence-spending>

About the Authors

Preston Feinberg

Preston Feinberg leads congressional engagement for Palantir's Air Force, Army, and Space Force programs. He has over a decade of experience in Washington, D.C. working on national security policy, congressional affairs, and strategic advocacy across the aerospace and defense sectors. Preston was previously the U.S. Air Force and F-35 Operations Lead at Lockheed Martin Government Affairs where he oversaw program management, business operations, and the team's consultants. Earlier in his career, he served as a Legislative Analyst for the U.S. Air Force appropriations liaison office, where he prepared senior civilian and uniformed leadership for engagements with congressional appropriators. Preston also worked at the British Embassy, where he advised the UK Ambassador, Defense Attaché, and Ministry of Defence staff on U.S. defense policy and the annual National Defense Authorization Act (NDAA). Before that, he spent 3 years at The McKeon Group, the firm of former Chairman of the House Armed Services Committee, Buck McKeon, where he led legislative strategies for across the aerospace and defense sector. Preston's first job in the nation's capital was working at Cafe Milano in Georgetown while he interned with Senator Tom Udall (NM), Rep. Adam Smith (WA-9), and the Bipartisan Policy Center. Preston earned his bachelor's degree in political science from the University of South Carolina and received his master of arts in strategic studies from Johns Hopkins University.

Matthew Ferren

Matthew Ferren is an international affairs fellow in national security, sponsored by Janine and J. Tomilson Hill, at the Council on Foreign Relations

(CFR). He has extensive expertise in cybersecurity, military operations, and emerging technologies. At CFR, Mr. Ferren's research examines China's cyber programs, U.S. defense policy, and international cyber cooperation. Before joining CFR, he served in the Office of the Under Secretary of Defense for Policy, where he developed Department of Defense strategies, policies, and plans for employing military cyberspace operations to advance U.S. national security interests and counter major cyber threats. Beginning in 2021, Mr. Ferren helped stand up the White House Office of the National Cyber Director and coauthored the 2023 National Cybersecurity Strategy. He previously worked at the Department of the Treasury and at the U.S. Cyberspace Solarium Commission. Mr. Ferren holds a BA in political science from Bates College and an MA in security studies from Georgetown University's Walsh School of Foreign Service.

Bonnie S. Glaser

Bonnie S. Glaser is managing director of GMF's Indo-Pacific program. She is also a nonresident fellow with the Lowy Institute in Sydney, Australia, and a senior associate with the Pacific Forum. She is a co-author of *US-Taiwan Relations: Will China's Challenge Lead to a Crisis* (Brookings Press, April 2023). She was previously senior adviser for Asia and the director of the China Power Project at the Center for Strategic and International Studies. Glaser has worked at the intersection of Asia-Pacific geopolitics and US policy for more than three decades.

From 2008 to mid-2015, she was a senior adviser with the CSIS Freeman Chair in China Studies, and from 2003 to 2008, she was a senior associate in the CSIS International Security Program. Prior to joining CSIS, she served as a consultant for various U.S. government offices, including the Departments of Defense and State. Ms. Glaser has published

widely in academic and policy journals, including the Washington Quarterly, China Quarterly, Asian Survey, International Security, Contemporary Southeast Asia, American Foreign Policy Interests, Far Eastern Economic Review, and Korean Journal of Defense Analysis, as well as in leading newspapers such as the New York Times and Wall Street Journal and in various edited volumes on Asian security. She served as a member of the Defense Department's Defense Policy Board China Panel in 1997. Ms. Glaser received her B.A. in political science from Boston University and her M.A. with concentrations in international economics and Chinese studies from the Johns Hopkins School of Advanced International Studies.

Sonia Horonziak

Sonia Horonziak is Doctor of political science and administration and Director of the Democracy and Civil Society Program at the Institute of Public Affairs, Poland. Lecturer at the University of Warsaw. Graduate of the Jagiellonian University in Krakow and a research scholarship program at the Technische Universität Dresden, Germany. In the years 2020-2023, she worked as a Specialist for Scientific Contacts at the Polish Academy of Sciences – Scientific Centre in Vienna. Until 2018, she was an acting president of the Polish Foundation for Education of Polish Children Living Abroad (pol. Fundacja Edukacji Polonijnej). For years, she has been cooperating with scientific institutions and NGOs in Poland and abroad by promoting Polish research, supporting education among Polish children in different countries and establishing international scientific contacts with multiple European organizations. Author of many publications in the field of political polarization, democratic theory and electoral processes. She is fluent in English and German.

Daria Impiombato

Daria Impiombato researches elite politics and party-state structures, domestic security, societal resilience and human rights in China, as well as the PRC's communication strategies and global information and influence operations. Her work explores how the party state exercises, safeguards and projects political power across institutions and society, as well as in China's engagement with counterparts abroad. Before joining MERICS, Impiombato worked as an analyst at the Australian Strategic Policy Institute's (ASPI) Cyber, Technology and Security team. Her research areas included human rights and technology, state policy in minority areas and foreign information operations and interference.

Lauren Kirby

Lauren Kirby is the Director of Strategy and Design at Democracy International. In her role, she leads the strategy and design team through her technical expertise on democracy, human rights, and governance policy and program issues. Ms. Kirby's expertise specifically focuses on civil society and civic activism, independent media, workers' rights, elections, political processes, and inclusive development. Prior to joining DI, she was the Civil Society, Labor, and Media Office Director in USAID's Bureau for Democracy, Human Rights, and Governance, where she led technical teams in innovative program design and formation of U.S. government policy priorities. Ms. Kirby joined USAID in 2011 as a Presidential Management Fellow. Over her 12 years with USAID, she worked in multiple DC-based bureaus and overseas missions, including Liberia, South Sudan, and the Regional Development Mission for Asia. She was one of the pioneers behind USAID's Women in Power learning activity, which presents programmatic best practices for measuring and increasing women's political participation. Ms.

Kirby has a Bachelor of Arts in Political Science and Philosophy from Boston College and a Master of Public Policy in International Policy and Development from Georgetown University's McCourt School of Public Policy.

Filip Krenek

Filip Krenek is a Project Coordinator and Analyst at EUROPEUM Institute for European Policy in Prague. He focuses on European economy, competitiveness, and economic security, with expertise in the automotive, steel, and battery sectors as well as supply chains and critical raw materials. Before joining EUROPEUM in 2024, he worked at the European Commission in Brussels (DG Competition, DG Trade, DG Regio) and was a James S. Denton Fellow at CEPA in Washington, DC. He regularly publishes policy reports, papers and briefs and comments on EU affairs in Czech and international media.

Jacqueline Ramos

Jacqueline Ramos is a foreign policy professional with extensive experience shaping U.S. engagement in Europe. She most recently served as Deputy Assistant Secretary of State in the Bureau of European and Eurasian Affairs, leading policy toward Western Europe and the European Union. Previously, she was Senior Professional Staff Member for Europe and Russia on the U.S. House Foreign Affairs Committee and an adjunct fellow at the Center for a New American Security. She has held positions at the Department of Defense, the National Nuclear Security Administration, and Airbus Group. She holds degrees from St. Olaf College, Georgetown University, and Johns Hopkins SAIS.

Colleen Scribner

Colleen Scribner is deputy director of the Indo-Pacific Program at GMF. Prior to joining the organization, she served as senior program manager for Asia programs at Freedom House, where she led strategy and oversaw human rights and democratic resilience programming across the region. Before that, she worked on Freedom House's Emergency Assistance Program, rising from senior program associate to program manager. She designed and implemented rapid response grantmaking, civil society protection, and socio-political change programs for at-risk civil society organizations and human rights defenders in restrictive environments globally. She has also held roles at the Public International Law and Policy Group and the Global Fund to End Modern Slavery.

Scribner was a 2023 Penn Kemble Fellow at the National Endowment for Democracy and the 2020 Young Professionals in Foreign Policy Rising Experts Human Rights Fellow. She holds a master's degree from American University's School of International Service in global governance, politics, and security and a bachelor's degree from Occidental College in diplomacy and world affairs.

Ulf Steindl

Ulf Steindl is Senior Research Fellow with the Austrian Institute for European and Security Policy (AIES), where he has worked since May 2022. His expertise centres on issues of European and Transatlantic Security, as well as geopolitical competition. Ulf's research currently focuses on policy analysis and politico-military aspects of the European Defence Technological and Industrial Base (EDTIB), EU-NATO complementarity, and the EU's Common Security and Defence Policy (CSDP). This includes the analysis of current crises directly related to the discussion on European Security and Defence, such as Russia's war

against Ukraine. Additionally, Ulf's expertise extends to the East Asian region, particularly in geostrategy, defence industry, and defence innovation in China, Japan, and South Korea. Ulf earned his Bachelor's degrees in Geography and Political Science, and obtained a Master's degree in East Asian Economy and Society from the University of Vienna. He also completed a Master of Advanced International Studies (M.A.I.S.) at the Diplomatic Academy of Vienna. His academic journey included semesters abroad in Vietnam and South Korea. During this period, Ulf also worked for an FDI consulting agency in China.

Rachel Vandenbrink

Rachel Vandenbrink is a researcher at the Institute for Defense Analyses, where she focuses on U.S. defense partnerships and security dynamics in the Indo-Pacific, and a collaborator with the Southeast Asia Peace Institute. Previously, she was a Southeast Asia Policy Advisor at the U.S. Department of Defense from 2022 to 2025, where she served as Country Director for Burma, Brunei, Cambodia, Indonesia, and Singapore and provided policy analysis on regional priorities and defense cooperation. As a program officer at the U.S. Institute of Peace, she managed research and dialogue programs focused on U.S.–China competition and supported the expansion of the Institute's programming in East and Southeast Asia. She also reported on human rights and political developments in East and Southeast Asia as an editor at Radio Free Asia and held short-term roles with the International Crisis Group in Beijing and the Congressional–Executive Commission on China. Rachel holds a Master of Arts in Law and Diplomacy from The Fletcher School at Tufts University, with concentrations in Security Studies and East Asian Studies, and a Bachelor of Arts in History and East

Asian Studies from the University of Chicago. She is proficient in Mandarin Chinese and Japanese.

Thomas Yoshimura

Thomas Yoshimura became Policy Advisor China at Konrad-Adenauer-Stiftung (KAS) headquarters in Berlin in August 2025. Having joined KAS in 2011, he started as Project Manager in the then established Representative Office in Tokyo. In 2014, he was transferred to Jakarta as Assistant Representative and Acting Director of the KAS Office for Indonesia and Timor-Leste. After two years, Thomas returned to Berlin and was briefly in charge of ECM Training Management. In 2019 he became responsible for the Desk for Japan, Korea, Australia, New Zealand and the Pacific. Between August 2020 and July 2025, he lastly served as Resident Representative in Korea, where his work focused on perceptions and developments of the global and regional security order as well as to autonomous driving and all matters related to a sustainable mobility transformation across the Indo-Pacific under the pillar of innovation. Thomas studied at the University Duisburg-Essen and the Ryukoku University in Kyoto and holds a Diploma in East Asian regional studies.

G | M | F