Institute for National Defense and Security Research
Volume 15 I Issue 1 I June 2026 I ISSN 2

DEFENSE SECURITY BRIEF

THE INSTITUTE FOR NATIONAL DEFENSE AND SECURITY RESEARCH (INDSR)

The Institute for National Defense and Security Research (INDSR) is dedicated to fueling knowledge-based policy analyses and strategic assessments on Taiwan's security. Our mission is to safeguard Taiwan's democracy and prosperity by strengthening mutual understanding and advancing common interests in the defense and security community both domestically and internationally. INDSR was formally inaugurated on May 1, 2018, and is headquartered in Taipei, Taiwan. We are an independent, nonpartisan, nonprofit organization.

To bring together great minds in policymaking, industry and research, we convene international forums, network civil societies, engage in Track Two dialogue and conduct wargame simulations. INDSR's dynamic research agenda and activities are used to develop pragmatic policy recommendations for the government of Taiwan.

DEFENSE SECURITY BRIEF

Defense Security Brief (DSB) is an English-language publication aimed at strengthening research exchanges with security-related experts both domestically and abroad. Established in 2011, DSB was originally founded and compiled by the Office of Defense Studies, Ministry of National Defense. INDSR continued the publication in 2018.

OFFICE

Institute for National Defense and Security Research
No.172, Bo-Ai Road, Zhongzheng Dist., Taipei City, Taiwan (R.O.C.)
Tel: 886-2-2331-2360 Ext.705 | Fax: 886-2-2331-2361
Printed in Taiwan
ISSN 2225360-2

Taiwan's Maritime Security: A European Perspective*

*Dr. Heiko Herold***

Taiwan's maritime security is shaped by its dependence on maritime trade, its proximity to an increasingly assertive and aggressive China, and the need to protect its critical sea lines of communication. This article focuses on the core aspects of Taiwan's maritime security by outlining its strategic importance, analyzing the nature of maritime threats posed by China, identifying Taiwan's key vulnerabilities at sea, and assessing the measures Taiwan is taking to deter and counter Chinese aggression in the maritime domain.

I. STRATEGIC IMPORTANCE OF TAIWAN'S MARITIME SECURITY

Why does Taiwan's maritime security matter? It is of great importance because it protects the sovereignty of a thriving democracy at a strategic crossroads, it safeguards vital sea lanes and submarine infrastructure crucial for global trade and semiconductor supply chains, and it helps maintain peace and stability in the Indo-Pacific region in the face of China's continued military pressure and gray-zone aggressions. This security effort addresses a wide range of challenges including naval intimidation and the risk of blockades, cyber warfare, legal disputes, and coercive gray-zone tactics designed to undermine Taiwan's control over its maritime zones and threaten its vital ports, sea lines of communication, and critical seabed infrastructure. It also strengthens Taiwan's role as a crucial pillar for maintaining the regional order and preventing disruptions to the global economy.

---

* This article is a revised version of my keynote on "Taiwan's Maritime Security" at the 4th Berlin Taiwan Conference on December 4, 2025.

** Heiko Herold is Non-Resident Fellow at the Institute for Security Policy at Kiel University. He is a German historian and security policy analyst, and holds a PhD in history from Düsseldorf University. He has worked as a policy advisor and public affairs manager for the U.S. Department of State, the German Armed Forces, non- governmental organisations, and several companies in Germany, the Balkans, China and South Asia. He holds the rank of Commander in the German Navy Reserve. His research interests include transatlantic foreign and security policy, maritime security in Europe and the Indo-Pacific, transatlantic China policy, and hybrid warfare.

Taiwan holds a crucial strategic location in the Indo-Pacific region due to its position within the "first island chain," which stretches from Japan through Taiwan to the Philippines and down to Borneo. This island chain is key to controlling access between the East and South China Seas and beyond to the Pacific and Indian Oceans. Taiwan functions as a maritime gateway, controlling vital sea lanes essential for global trade and military logistics, particularly connecting Northeast Asia with the markets of Europe and the Middle East. Taiwan's geographic significance extends to its relations with its neighbors, making the island a central point in the regional security dynamics between China, the United States, Japan, and other Indo-Pacific powers. The island's location limits China's access to the Pacific Ocean, thereby impacting its maritime expansion ambitions and strategic deterrence capabilities, especially regarding submarine operations and ballistic missile forces.

The waters surrounding Taiwan are a focal point of strategic and geopolitical tensions. They encompass the East China Sea to the north, the Taiwan Strait to the west, the South China Sea to the south, and the Pacific Ocean to the east. The Taiwan Strait, a vital international waterway connecting the East and South China Seas, is a crucial maritime route for trade and military movements. China claims it as part of its internal waters, but this position has no legal basis; it contradicts international law and violates the United Nations Convention on the Law of the Sea, or UNCLOS, including provisions guaranteeing freedom of navigation. China's aggressive maritime claims extend throughout these and adjoining waters, especially under the umbrella of the expansive and internationally disputed "ten-dash line", which includes nearly 90% of the South China Sea and overlaps with territorial claims by Taiwan and several Southeast Asian nations. This claim is also illegal under international law. In 2016, an UNCLOS arbitration tribunal definitively rejected China's fabricated historical claims to these waters, ruling that they lacked any legal or factual basis.[1] Nevertheless, China is pursuing these claims through gray-zone warfare, military presence, lawfare, and land reclamation projects for military purposes to consolidate its control and restrict access to the South China Sea. In response, the United States and regional actors such as the Philippines and Japan are deepening their naval and other military cooperation, for example, through defense pacts and recent naval exercises in the South China Sea, to strengthen joint maritime security and counter China's hegemonic power ambitions. These enhanced partnerships reflect growing concerns about China's increasing influence

1. Permanent Court of Arbitration, "The South China Sea Arbitration," *The Hague*, July 12, 2016, https://pca-cpa.org/en/cases/7.

and support freedom of navigation and regional security in these disputed waters.

II. CHINA'S THREATS AGAINST TAIWAN

China is posing a growing challenge to Taiwan through explicit threats of forcible annexation, misleadingly framed as "reunification," even though Taiwan has never been part of the People's Republic of China. Beijing's strategy aims to conquer Taiwan without firing a shot, that is through gray-zone tactics designed to weaken its defenses, normalize border violations, deplete resources, and force Taiwan to surrender through economic strangulation, disinformation, and psychological pressure. In the maritime domain, these gray-zone operations include severing submarine cables vital to Taiwan's economy and military, cyberattacks on critical infrastructure, and the Chinese Coast Guard's alleged "law-enforcement" in waters around Taiwan's outlying islands.

Chinese forces regularly intrude into Taiwan's maritime borders as well as its air defense identification zone beyond the median line with hundreds of incursions per month using military aircraft, naval vessels, and drones. The aim of these actions is to weaken Taiwan's reactive capabilities and test its response times. The People's Liberation Army regularly conducts large-scale exercises around Taiwan, practicing joint blockade operations, amphibious landings, and missile strikes to refine invasion tactics and signal a readiness for rapid escalation. Underpinning these efforts is China's rapid naval expansion—now the world's largest fleet by number, including aircraft carriers and nuclear submarines—and the comprehensive modernization of its air force, focusing on stealth fighters, long-range bombers, unmanned aerial systems and drones. All of this is designed to achieve naval and air superiority in a potential conflict and deter U.S. intervention.

III. TAIWAN'S KEY VULNERABILITIES IN THE MARITIME SECURITY DOMAIN

What are Taiwan's key vulnerabilities in the maritime security domain that China could exploit in a crisis or wartime scenario? As a densely populated island with limited natural resources, it is heavily dependent on maritime imports, particularly regarding energy, food, raw materials, chemicals, and military equipment. The most significant maritime export dependencies are concentrated on high-value industrial goods, particularly electronics, which make up over 40 percent of exports.[2] Most of

2. "Trading Economics: Taiwan Exports YoY," https://tradingeconomics.com/taiwan/exports-yoy.

Taiwan's imports and exports by sea move through a small number of major ports such as Kaohsiung, Taichung and Taipei, which together handle tens of millions of containers and hundreds of billions of U.S. dollars in trade each year. This intense port activity is large even relative to Taiwan's overall GDP, underscoring how central seaborne trade is to its economy.[3] Therefore keeping access to regional and global sea lanes is framed as "critical to national survival."[4]

Energy is one of Taiwan's sharpest vulnerabilities, since the island has virtually no domestic fossil fuel production and relies almost entirely on seaborne imports of oil, coal, and especially liquefied natural gas to power its industries and cities. Any sustained disruption to shipping routes or port operations would therefore quickly affect electricity generation, industrial output, and living standards.

Taiwan also relies on maritime imports for a significant portion of its food supply, reflecting a high degree of dependency on global markets for agricultural and food products. In recent years, its food self-sufficiency rate has dropped to roughly 30 percent. While Taiwan maintains high self-sufficiency in some sectors—such as rice—its reliance on maritime imports is especially acute for meat, animal feed, seafood, and high-value processed foods. Taiwan has stockpiled food supplies for several months. However, any disruption to sea lanes would quickly impact the island's ability to secure a wide variety of food products, underscoring the close link between its food security and the stability of maritime trade routes.[5]

Taiwan also depends heavily on seaborne deliveries for major military platforms, spare parts, and advanced components, because most of its high-end defense equipment is imported, above all from the United States. Complex systems such as fighter aircraft, air-defense missiles, precision-guided munitions, and many critical subsystems for indigenous weapons programs all arrive by ship or rely on maritime

---

3. Kenan Arkan, Isaac A. Harris, Mark Montgomery, Peter Olive, Craig Singleton, "Maritime Protection of Taiwan's Energy Vulnerability," *FDD*, 2025, https://www.fdd.org/analysis/2025/11/17/maritime-protection-of-taiwans-energy-vulnerability; Matthew P. Funaiole, Brian Hart, David Peng, Bonny Lin, Jasper Verschuur, "Crossroads of Commerce: How the Taiwan Strait Propels the Global Economy," *CSIS*, 2024, https://features.csis.org/chinapower/china-taiwan-strait-trade; Tiffany Lee, "Taiwan Ports Guide 2025: Kaohsiung, Taichung & More," *FreightAmigo*, 2025, https://www.freightamigo.com/en/blog/logistics/exploring-taiwans-strategic-ports-a-comprehensive-guide-for-shippers.

4. "2013 Quadrennial Defense Review," *Taiwan Ministry of National Defense*, 2013, p. 39, https://www.ssri-j.com/MediaReport/Document/TWQDR2013.pdf.

5. Ethan Dean-Richards, "Taiwan's Food Security Poses a Risk to Its National Security," *Domino Theory*, Taipei 2025, https://dominotheory.com/taiwans-food-security-poses-a-risk-to-its-national-security; "2024 Taiwan Agricultural Exports Summary," *U.S. Department of Agriculture*, 2025, https://apps.fas.usda.gov/newgainapi/api/Report/DownloadReportByFileName?fileName=2024+Taiwan+Agricultural+Exports+Summary_Taipei_Taiwan_TW2025-0005.pdf.

logistics at some stage. Against this background, Taiwan has for many years imported large quantities of military stockpile. The main supplier is the United States, and that remains the case under the second Trump administration. In mid-November 2025, the U.S. Department of State has approved a 330 million U.S. dollar Foreign Military Sales package providing non-standard spare parts and support services for Taiwan's F-16, C-130, and Indigenous Defense Fighter fleets.[6] Nonetheless, any blockade or serious disruption of commercial shipping could quickly affect Taiwan's ability to sustain operations, replace losses, and keep its armed forces supplied over time.

Taiwan's export model also ties its prosperity to secure sea lanes, particularly for semiconductors and other electronics that dominate its trade profile. Taiwanese companies produce the vast majority of the world's most advanced chips and many other electronics, and lots of these components leave the island by ship to feed global manufacturing and digital infrastructure. For this reason, a naval blockade or war over Taiwan would not only affect the island's economy but would also have repercussions for global supply chains.

IV. TAIWANESE COUNTERMEASURES AGAINST CHINESE AGGRESSION

Taiwan counters Chinese aggression through what once was called "Overall Defense Concept," a doctrine emphasizing "agile response capabilities and whole-of-society defense resilience," as stated in the 2025 Quadrennial Defense Review.[7] Its core objective is to build a force that can foil the enemy by employing asymmetric warfare, mobility, and denial strategies to survive initial assaults and impose high costs on invaders. Military modernization drives this effort, with President Lai Ching-te announcing in his 2025 National Day speech a special budget to push defense spending above 3% of GDP immediately and to 5% by 2030, funding the indigenous "T-Dome" multi-layered air defense system for "high-level detection and effective interception," alongside Hai Kun submarines, Tien Kung III missiles, and mass drone production.[8] The 2025 National Defense Report reinforces "layered deterrence" and

---

6. Kanishka Singh, "US Approves Potential $330 Million Arms Sale to Taiwan, First under Trump," *Reuters*, November 14, 2025, https://www.reuters.com/business/aerospace-defense/us-state-dept-approves-possible-sale-taiwan-fighter-jet-spare-repair-parts-2025-11-14.

7. "Republic of China 114th Year Quadrennial Defense Review 2025," *Taiwan's Ministry of National Defense,* 2025, p. 6, https://tsm.schar.gmu.edu/wp-content/uploads/2025/03/Taiwans-2025-QDR.pdf; Tamir Eshel, "TADTE 2025: Reflecting Taiwan's Strategic Themes," *Defense Update*, September 22, 2025, https://defense-update.com/20250922_tadte-2025-reflecting-taiwans-strategic-themes.html.

8. "President Lai Delivers 2025 National Day Address," *Office of the President*, October 10, 2025, https://english.president.gov.tw/News/7022.

"resilient defense," integrating intelligence, surveillance and reconnaissance assets like radars, unmanned aerial vehicles, and reserves for "multi-domain denial," with the annual Han Kuang exercise simulating a Chinese blockade and invasion and practicing rapid mobilization.[9]

Taiwan bolsters its maritime domain awareness and counters Chinese claims through expanding international cooperation, hosting forums like the 2025 Taiwan International Ocean Forum where President Lai emphasized working "with democratic partners throughout the world in a maritime spirit of freedom and openness to contribute to ocean governance and jointly ensure maritime security."[10] The U.S. National Defense Authorization Act for Fiscal Year 2026 authorizes deepened U.S. Coast Guard training with Taiwan's Coast Guard Administration on maritime security and law enforcement and directs the U.S. Department of War "to engage with Taiwan to develop a joint program to co-develop and co-produce uncrewed and counter-uncrewed capabilities."[11] Taiwan pursues joint patrols and intelligence-sharing with Japan and the Philippines amid South China Sea tensions, and invests in unmanned surface vessels and AI surveillance according to the 2025 National Ocean Policy White Paper to address gray-zone threats like illegal fishing and seabed infrastructure sabotage, demonstrating a shift from unilateral defense to multilateral deterrence.[12]

In practice, Taiwan intercepted and charged the captain of the Togolese-flagged cargo vessel "Hong Tai 58," crewed by Chinese nationals, in February 2025 for deliberately severing a submarine cable off its southwest coast—the first such prosecution— arrested the crew, escorted the ship for investigation, and increased coast guard patrols to counter gray-zone sabotage.[13] Taiwan continuously monitors incursions by People Liberation Army aircraft, deploying combat air patrol fighters such as F-16s for identification and interception, but these are carefully calibrated responses to avoid escalation. Coastal missile systems and naval assets also

---

9. "ROC National Defense Report 2025," *ROC Ministry of National Defense*, 2025, https://www.mnd.gov.tw/newupload/ndr/114/114ndreng.pdf.
10. "President Lai, Meets Delegation from 2025 Taiwan International Ocean Forum," *Office of the President*, July 1, 2015, https://english.president.gov.tw/News/6982.
11. "National Defense Authorization Act for Fiscal Year 2026," *United States Senate Committee on Armed Services*, 2025, https://www.armed-services.senate.gov/imo/media/doc/fy2026_ndaa_executive_summary.pdf.
12. "2025 National Ocean Policy White Paper," *Ocean Affairs Council,* 2025, https://www.oac.gov.tw/filedownload?file=publication/202509251242090.pdf&filedisplay=2025oceanwp-0925.pdf&flag=doc.
13. Koh Ewe, I-ting Chiang, "Taiwan Jails China Captain for Undersea Cable Sabotage in Landmark Case," *BBC*, June 12, 2025, https://www.bbc.com/news/articles/cwy3zy9jvd4o].

track and prepare to counter threats. Taiwan has also proposed forming a "National Defense Innovation Task Force" as part of its 2025 Quadrennial Defense Review to prioritize areas like unmanned systems, counter-unmanned systems, and AI applications, including for its naval forces.[14]

V. LOOKOUT: HOW LIKELY IS A BLOCKADE OR INVASION OF TAIWAN?

The question of how real a Chinese attack on Taiwan is in the near future is a concern for politicians, military leaders, and analysts worldwide. Numerous warnings from the U.S., Japan, Taiwan itself, and other partner countries underscore the heightened risk in the coming years. The year 2027 is repeatedly mentioned, a symbolically and politically significant date: the 100th anniversary of the People's Liberation Army and a target year by which China intends to have fully modernized its armed forces. According to U.S. intelligence estimates, "Xi has ordered his military to be ready for a military takeover of Taiwan by 2027."[15] President Xi Jinping has repeatedly stated his intention to resolve the "Taiwan question" during his lifetime. Unlike Deng Xiaoping, he understands so-called "reunification" not as a long-term process, but as a political legacy. This adds further political pressure to the issue.

China has been intensifying its military preparations for years, some visibly, some covertly. These include the large-scale modernization of its navy, the gradual maritime encirclement of Taiwan, extensive hybrid operations, and increasingly realistic exercises simulating blockades and invasion scenarios. Hybrid warfare is already in full swing, with submarine cable sabotage, disinformation, cyberattacks, and economic pressure. The military refers to this as shaping the battlefield.

The situation is also geopolitically dangerous due to a changed strategic environment: Many observers consider a Chinese attack on Taiwan during Donald Trump's second term in office realistic. From Beijing's perspective, a U.S. president who unsettles allies and questions multilateral structures could reduce the costs of a Chinese military intervention. Xi Jinping has repeatedly and publicly affirmed China's commitment to peace. We should not be fooled. China's intense hybrid war against Taiwan and its unmistakable preparations for a kinetic war tell a different story.

---

14. Taiwan Security Monitor and Eric Gomez, "Republic of China 114th Year Quadrennial Defense Review 2025," March 19, 2025, p. 6, https://tsm.schar.gmu.edu/wp-content/uploads/2025/03/Taiwans-2025-QDR.pdf.

15. Yaroslav Trofimov, "A Newly Confident China Is Jockeying for More Global Clout as Trump Pulls Back," *Wall Street Journal*, February 12, 2025, https://www.wsj.com/world/china/a-newly-confident-china-is-jockeying-for-more-global-clout-as-trump-puls-back-5cc3be4e.

At the same time, many experts emphasize that China is not yet ready for a large-scale military operation against Taiwan. Added to this are economic challenges, domestic political pressure, and uncertainty about the reactions of the U.S. and its partners. The so-called "four-front argument," which was rolled out in Chinese propaganda in 2023, illustrates the geopolitical complexity that would make a full-scale war risky for China. According to this argument, China faces the threat of war on four fronts simultaneously: Taiwan, the South China Sea, the border with India, and, particularly noteworthy, Korea. While the four-front argument was intended to appease war hawks in China, it also underscores that, according to Chinese military planners, a war over Taiwan would most likely not be a limited war.[16]

However, we cannot rely on China only daring to attack Taiwan when its military is supposedly ready for it. Furthermore, an attack would not necessarily have to begin with a full-scale invasion. More likely are escalating preliminary stages: for example, the blockade of individual ports, the disruption of critical sea lines of communication, and military "test attacks" on Taiwanese offshore islands such as Pratas, Taiping, Kinmen, or Matsu.

How can an attack be prevented? The most important factor is deterrence, specifically a deterrence that, from a Chinese perspective, is so costly that it would threaten the very core of the Communist Party. What Xi and party leadership fear most is not just a military fiasco, but an attack that ends in chaos and endangers the regime itself. This requires three core elements:

1. Taiwan needs strong and reliable alliances, above all with the United States and Japan, complemented by a deepening cooperation with Australia, the Philippines, and key European partners.
2. Maximum resilience for Taiwan: militarily, economically, digitally, and societally, to withstand and recover from sustained pressure or disruption.
3. Taiwan needs credible defense capabilities including asymmetric systems, multi-domain denial, robust maritime defenses, protection of critical infrastructure, and high mobilization capacity.

Finally, I would like to address one last important point: We must not consider the Taiwan issue in isolation. We are already in the midst of a systemic rivalry between autocracies and democracies. Taiwan, Ukraine, and Israel are fighting

16. Katsuji Nakazawa, "Analysis: China's Messaging Machine Tamps down Taiwan War Hype," *Nikkei Asia,* May 11, 2023, https://asia.nikkei.com/editor-s-picks/china-up-close/analysis-china-s-messaging-machine-tamps-down-taiwan-war-hype.

on the front lines. The hybrid war waged by the autocracies is directed against the global West, and it is continuously intensifying. Further kinetic wars are looming on the horizon, and it is unclear whether they can be prevented. If the autocrats have their way, the international rules-based order will be replaced by a multipolar world order, which means nothing other than exclusive spheres of influence for a few major powers. In the Indo-Pacific, this means: China wants to take control of Taiwan and push the Americans out of the Pacific in order to dominate the region. But the Chinese Communist Party is already thinking further ahead and dreams of a Sinocentric world order. One remark Xi Jinping made to Vladimir Putin in March 2023 was particularly revealing, as it highlighted both the scale of the current global upheavals and the deliberate intention behind them: "Right now there are changes – the likes of which we haven't seen for 100 years – and we are the ones driving these changes together."[17]

Therefore, from a European perspective, it is in our own best interest, not only for economic but above all for geostrategic reasons, to do everything possible to support Taiwan in its defensive measures against the increasingly aggressive and belligerent People's Republic of China with our democratic allies worldwide and to prevent a Chinese takeover of the island republic.

17. Al Jazeera, "China's Xi Tells Putin of 'Changes Not Seen for 100 Years'," March 22, 2023, https://www.aljazeera.com/news/2023/3/22/xi-tells-putin-of-changes-not-seen-for-100.

Taiwan in India's Indo-Pacific

*Dr. Manoj Kumar Panigrahi**

India's Act East policy approaches can be seen as an extension of its policies in the Indo-Pacific region, with Southeast Asia as its core.[1] It was initially developed under its "Look East" policy in 1991 to bring Southeast and East Asian countries into its policy outlook. The major scope of the India's Indo-Pacific vision extends from the eastern coast of Africa to the western Pacific Ocean region which includes both maritime and continental dimensions. The key pillars to such vision first lies at "Free, Open, and inclusive Indo-Pacific (FOIP)" which means respect the International Law primarily the United Nations Convention on the Law of the Sea (UNCLOS), second, it is to support its security and strategic cooperation and economic engagement in the region, thirdly, connectivity and development which includes issues such as climate change and cultural connections.

However, on many occasions, Taiwan has been missing from the Act East policy outlook. The reason is India's own policy of recognizing the People's Republic of China (PRC) as the sole stakeholder of Mainland China in 1950.[2] This policy has led to the de-recognition of the Republic of China (ROC) as the representative of the mainland. Since the ROC government moved to Taipei in 1949 and India recognised the PRC, the ROC has received no further engagement. It has gradually diminished in policy circles in New Delhi. With India's strategic relationships with Japan and South Korea and booming trade, India's trade in the region has gradually increased. This article will introduce the recent debates on increasing India's relations with Taiwan amid strained India-China relations.

---

* Dr. Manoj Kumar Panigrahi is currently an Associate Professor and co-Director of the Centre for Northeast Asia Studies, in Jindal School of International Affairs at O.P. Jindal Global University. He is currently a MOFA Visiting Fellow, Taiwan at National Chengchi University. He teaches courses on Taiwanese History and Politics, Cross-strait relations, East Asian Politics.

1. "Question No-1456 India's Act-East Policy," *MEA-India*, July 28, 2023, https://www.mea.gov.in/lok-sabha.htm?dtl/36927/QUESTION+NO1456+INDIAS+ACTEAST+POLICY.

2. *Ibid*.

India's engagement in the region can be grasped through several angles. Historically, the countries in the region, primarily with Japan and South Korea, have been long-term partners of India. New Delhi has been involved in the Tokyo trials to bring justice after World War II and has also played a key role in providing humanitarian assistance during the Korean War. Given a strong presence of both Korean and Japanese companies in India, the bilateral relations have increased significantly on all sides. As per the trade data (see Table 1), India's trade in the region has seen significant growth potential. The data below reflect exports from India, Japan, South Korea, China, and Taiwan to each other. Table 1 helps us understand the massive trade flows India has with East Asian countries, including Taiwan, known for its semiconductor prowess.

Table 1: Number of exports in billion USD in the year 2024

	India	Japan	South Korea	China	Taiwan
India		5.73	5.88	14.9	2.714
Japan	18.36		46.38	125	46.5
South Korea	18.66	29.6		132.9	38.7
China	120.46	152.01	146.23		77.5
Taiwan	7.89	25.8	28.7	105	

Source: Author compilation from open sources.[3,4,5]

Table 1 clearly shows that India-Taiwan trade is almost 10 billion USD, suggesting greater potential for further development. Currently, most trade between India and Taiwan is focused on electronics, machinery, semiconductors, and minerals.

Since 1991, India's refocus on Southeast and East Asia led to a fresh start of engagements with the region. This led to the gradual opening of India's relations

3. "Bilateral Trade," *Administration, International Trade*, March 6, 2026, https://www.trade.gov.tw/english/BilateralTrade/BilateralTrade.aspx?code=7030&nodeID=4618&areaID=2&country=SW5kaWE=.

4. "Japan Exports to India," *Economics Trading*, March 7, 2026. https://tradingeconomics.com/japan/exports/india.

5. "South Korea Exports," *Economics Trading*, March, 2026, https://tradingeconomics.com/south-korea/exports.

with Taiwan, which remained short of formal diplomatic ties but focused more on economic and cultural ties. In 1995, under a mutual agreement, both New Delhi and Taipei established offices that served as de facto embassies in each other's capitals. The Indian office is known as the India-Taipei Association (ITA), whereas Taiwan's office in New Delhi is presently called the Taipei Economic and Cultural Centre in India (TECC). By 2026, Taiwan has added two other offices in Mumbai and Chennai, marking a significant increase in its presence in India. The bilateral relations also got a boost since 2016 when Taiwan's former president Tsai Ing-wen initiated a refurbished policy named "New Southbound Policy (NSP)". Under NSP, India became one of the major countries with which Taiwan aimed to strengthen its relations. Similarly, India's Taiwan policy did not involve any specific policies towards Taiwan but rather a gradual opening of economic and technical cooperation.

The Taiwan Strait, along with the East Asian region, has become increasingly important to Indian policymakers. India has been a vocal observer of the rising tensions not only in its neighbourhood but also in other major potential flashpoints around the world, such as the South China Sea and the Taiwan Strait. India has been more actively voicing its concerns in the region since the Chinese military exercises around Taiwan in August 2022.[6] The military exercise followed Nancy Pelosi, Speaker of the United States House of Representatives, visiting Taiwan in August 2022.[7] India's response to the drill was showing concerns and urged avoiding any unilateral actions to change the status quo, de-escalation of tensions and efforts to maintain peace and stability in the region".[8] Since then, India has on multiple occasions raised concerns about the potential for conflict in the region.

India's concerns are genuine, as more than 10 per cent of its trade passes through the Taiwan Strait. As per a report by the Centre for Strategic and International Studies (CSIS), 14.70 per cent of India's imports and 13.60 per cent of its exports transit through the Taiwan Strait, valued at approximately 170 billion USD. This is significantly larger than the United States's 3.20 net imports and 2.70 per cent of its net exports, totalling 154 billion USD.[9]

---

6. Silvia Shih, Steven Yeo, Sylvia Lee, Yingyu Chen, Meg Wu, Maps: China's 72-hour 'Taiwan Blockade'," August 15, 2022, https://www.cw.com.tw/graphics/pelosi-visits-taiwan-en/index.html.
7. "US House Speaker Nancy Pelosi's Visit to Taiwan Fruitful; Underlines Staunch US Support for Taiwan," *MOFA-Taiwan,* August 3, 2022, https://en.mofa.gov.tw/News_Content.aspx?n=1328&s=98251.
8. "Transcript of Weekly Media Briefing by the Official Spokesperson," *MEA-India,* August 12, 2022, https://www.mea.gov.in/media-briefings.htm?dtl/35635/Transcript_of_Weekly_Media_Briefing_by_the_Official_Spokesperson_August_12_2022.
9. "Crossroads of Commerce: How the Taiwan Strait Propels the Global Econom," *CSIS*, October 10, 2024, https://features.csis.org/chinapower/china-taiwan-strait-trade/.

Taiwan has also gradually increased its investment in India. It now stands as India's 16th-largest trading partner and 12th-largest export destination. Taiwan's investments in 174 cases amount to 1573 million USD, whereas India's investments in Taiwan stood at 763 cases, resulting in 78 million USD in total.[10] Semiconductor giants such as Powerchip Semiconductor Manufacturing Corp (PSMC) and Foxconn from Taiwan have been investing in India and forming joint partnerships with Indian counterparts, resulting in massive employment for Indian workers.[11] These companies would be crucial in talent cultivation in India's semiconductor journey. Taiwanese companies can also become crucial partners for India's "Digital India" and "Make in India" initiatives, which align with a long-term approach to developing bilateral ties.

Strategically, Taiwan is also key to India's vision of a FOIP. India's policy of Security and Growth for All in the Region (SAGAR) also highlights Maritime Security as one of its pillars. India and Taiwan mutually share this vision. With China's growing assertiveness towards India on the land border, the Philippines in the ocean, and air and water incursions against Taiwan, and to some extent against Japan as well, these countries naturally face the same issues. Territorial disputes with China have led these countries to form partnerships in both multilateral and bilateral forums. Though Taiwan is not recognised as a country, it interacts through several Track 1.5 and 2 dialogues. India, a member of the Quadrilateral Security Dialogue (Quad), has voiced concerns about the importance of peace and stability in the region, although as a group it has not directly mentioned Taiwan or China.[12] This is largely due to India's own refusal to see Quad as a grouping against any other country. In its joint statements, the Quad has also emphasised peace and the maintenance of the status quo in the Taiwan Strait.

Both India and Taiwan are now members of the United States' "Pax Silica," a group of countries that holds that economic security is national security and vice versa.[13]

---

10. "Bilateral Trade (Taiwan-India Economic Relations)," *ITA-Taiwan*, October 14, 2025, https://www.trade.gov.tw/english/BilateralTrade/BilateralTrade.aspx?code=7030&nodeID=4618&areaID=2&country=SW5kaWE=.
11. Mondal, Shalini, "Foxconn Hires 30,000 Workers at Bengaluru iPhone Plant in Record Ramp-up: Report," *Excellence in AI Journalism*, December 22, 2025, https://analyticsindiamag.com/ai-news-updates/foxconn-hires-30000-workers-at-bengaluru-iphone-plant-in-record-ramp-up-report?trk=public_post_comment-text.
12. "Joint Statement from the Quad Foreign Ministers' Meeting in Washington," *Quad*, July 1, 2025, https://www.state.gov/releases/office-of-the-spokesperson/2025/07/joint-statement-from-the-quad-foreign-ministers-meeting-in-washington.
13. "United States and India Sign Pax Silica Declaration," *US-DoS*, February 20, 2026, https://www.state.gov/releases/office-of-the-spokesperson/2026/02/united-states-and-india-sign-pax-silica-declaration#:~:text=The%20United%20States%20welcomed%20India,Emirates%2C%20and%20the%20United%20Kingdom.

Though the agreement with Taiwan was more of an endorsement of the “Pax Silica Declaration,” it offers an opportunity for a platform where India and Taiwan, along with other like-minded countries, can work together to secure their economies, which are pooled in the alliance. With India’s large talent pool and Taiwan’s technological prowess, both sides can learn from each other and work on new technologies. India and Taiwan can also form partnership on developing sustainable energy from renewable energy sources. India being a growing economy needs large amount of energy whereas Taiwan in the past few years have been constantly facing energy crisis due to shutdown of its nuclear reactors. Both countries can work on energy such as solar, where India is a founding member of the International Solar Alliance. By knowledge sharing they can be mutually beneficial to each other and to the world.

All such developments have been crucial for India-Taiwan relations. Although non-diplomatically, both India and Taiwan's ties have surged ahead. There has been a growing number of people-to-people connections as well. The ties between India and Taiwan will largely be shadowed by India-China relations, given the complex geopolitical realities. It will be beneficial for the two sides to engage with each other and form partnerships through several non-political means.

China's Gray Zone Intrusions Against Taiwan

*Chauluen Lin**

INTRODUCTION

The geopolitical stability of the Indo-Pacific region, and Taiwan in particular, is currently facing a fundamental and unprecedented challenge from the People's Republic of China (PRC). China's persistent use of maritime gray-zone tactics poses a severe threat to regional stability and the international rules-based order. These actions are meticulously designed to achieve strategic aims—such as territorial advancement and the erosion of neighboring countries' sovereignty—without ever crossing the threshold into conventional armed conflict. By utilizing ambiguity and indirect coercion, China seeks to "advance without attacking", shaping a favorable strategic environment under the convenient guise of civilian or law enforcement activities.

To properly understand these intrusions, experts often refer to the "ICAD" framework introduced by U.S. Indo-Pacific Commander Admiral Samuel Paparo in 2024, which categorizes China's actions as Illegal (I), Coercive (C), Aggressive (A), and Deceptive (D).[1] China primarily executes these strategies through its national-level "Military-Civil Fusion" (MCF) strategy, a policy personally promoted by Chinese

---

* Retired Rear Admiral Chauluen Lin graduated from Naval academy and war college, served over 34 years in Taiwan's Ministry of National Defense (MND) and Coast Guard Administration (CGA). During his 32-year Navy career, he commanded four classes of warships and held key leadership roles, including Director of the Weapon Systems Division, Director of the Strategic Assessment Division, and Acting Director General of the Department of Integrated Assessment. He concluded his public service as CGA Chief Secretary, retiring on July 21, 2024. Now he is working for INDSR and his extensive expertise encompasses force building up, net assessment, cost analysis, foreign military sales, military-to-military engagement, and maritime domain awareness.

1. Yves-Heng Lim et al., *Assessing China's Grey Zone Tactics and Australia's Countervailing Options: The ICAD (Illegal, Coercive, Aggressive, Deceptive) Framework*, commissioned report (Department of Defence, Commonwealth of Australia, 2025), https://researchers.mq.edu.au/en/publications/assessing-chinas-grey-zone-tactics-and-australias-countervailing-/.

leader Xi Jinping. The core objective of the MCF strategy is to eliminate the barriers between the national defense sector and the civilian industrial and technological systems. This allows civilian assets to serve as a massive force multiplier for the military at a very low marginal cost, fundamentally blurring the lines between peace and war, and between civilian vessels and naval combatants.[2]

This report provides a comprehensive analysis of the recent patterns of Chinese gray-zone intrusions into Taiwan and surrounding regions, and subsequently details a robust, multi-layered framework of countermeasures that democratic nations must adopt to safeguard their sovereignty and regional peace.

I. RECENT PATTERNS OF CHINESE GRAY-ZONE INTRUSIONS

1. The Vanguard: Maritime Militia and Deceptive Fishing Fleets

A primary instrument in China's gray-zone playbook is the People's Armed Forces Maritime Militia (PAFMM), often referred to as China's "Little Blue Men" or the "Third Navy". This is a paramilitary force composed of vessels that appear to be engaged in civilian fishing but secretly collaborate with Chinese law enforcement and the military. The militia consists of two main types of vessels: specialized "Maritime Militia Fishing Vessels" (MMFV) built with military specifications, and "Spratly Backbone Fishing Vessels" (SBFV) which are heavily subsidized by the government to execute political missions.[3]

The militia frequently engages in deceptive practices to conceal its true intentions. For example, these boats often manipulate their Automatic Identification System (AIS) status, a tactic known as "going dark", and frequently change their ship names—sometimes over 1,000 times a year—to confuse international observers and avoid accountability.[4] Recently, highly organized and quasi-military behaviors have been observed among these fleets. In late 2025 and early 2026, thousands of Chinese fishing boats in the East China Sea abandoned normal fishing patterns and instead executed precise naval-style formations. On Christmas Day, approximately

2. Gregory B. Poling, Tabitha Grace Mallory, and Harrison Prétat, "Pulling Back the Curtain on China's Maritime Militia," *CSIS*, November 18, 2021, p. 12-16, https://www.csis.org/analysis/pulling-back-curtain-chinas-maritime-militia.

3. Andrew S. Erickson and Conor Kennedy, "Directing China's Little Blue Men: Uncovering the Maritime Militia Command Structure," *Asia Maritime Transparency Initiative*, September 11, 2015, https://amti.csis.org/directing-chinas-little-blue-men-uncovering-the-maritime-militia-command-structure/.

4. Lin Chauluen, "Confronting China's Pervasive Maritime Gray Zone Campaign," *SpaceNews,* October 30, 2025, https://spacenews.com/author/lin-chauluen/.

2,000 vessels formed a massive inverted “L” shape stretching 290 miles; shortly after, on January 11, 2026, over a thousand vessels formed a rectangular formation with a depth of 200 miles, maintaining these positions for up to 30 hours. These actions demonstrated a high level of command and control, effectively creating a physical barrier at sea that could disrupt international shipping lanes and delay the movement of adversary naval forces during a conflict.[5]

Taiwan faces direct threats from these deceptive vessels. In September 2023, the Taiwan Coast Guard intercepted a 600-ton steel vessel that had illegally entered Taiwan's territorial waters with its name erased. When ordered to stop, the vessel refused and deployed steel bars from its sides to violently resist boarding. After a forced boarding, the Coast Guard discovered 17 crew members equipped with high-tech communication gear, including satellite positioning systems, satellite phones, and facial recognition systems, proving the vessel was highly coordinated and connected to a larger command structure. These vessels are frequently used to test Taiwan’s defense resilience, gather intelligence, and potentially target critical underwater infrastructure such as submarine cables.[6]

2. The Weaponization of Dual-Use Civilian Shipping and RO-RO Ferries

Under the Military-Civil Fusion strategy, China is actively weaponizing large civilian shipping assets to bridge the gap in the People's Liberation Army’s (PLA) amphibious transport capabilities. Large Roll-on/Roll-off (RO-RO) ferries, originally built to military standards, serve as a vital component of this strategy.[7]

A prime example is the RO-RO ferry “Ji Long Dao”, which belongs to the Bohai Ferry Group and is considered part of the PLA’s maritime logistics reserve “Eighth Transport Squadron”. In 2023, this vessel participated in the PLA’s “Surge Lift Event Two”, transporting military vehicles and personnel from the Bohai Sea to designated ports like Qingdao, Rizhao, and Lianyungang. Between September and October 2025, “Ji Long Dao” displayed highly anomalous behaviors: after a prolonged period of extremely low-speed loitering near Dalian port, it suddenly executed a high-speed, long-distance southward voyage across multiple military theater commands,

5. Chris Buckley, Agnes Chang, and Amy Chang Chien, “Thousands of Chinese Fishing Boats Quietly Form Vast Sea Barriers,” *The New York Times,* January 16, 2026, https://www.nytimes.com/2026/01/16/world/asia/china-fishing-boats-barriers.html.

6. At the time of the incident, the author was serving as the chief secretary of the Taiwan Coast Guard Administration and was personally involved in handling the incident.

7. Lin, “Confronting China’s Pervasive Maritime Gray Zone Campaign,”.

traversing the Taiwan Strait and stopping at Xiaomo Port. During its southernmost transit, the vessel suspiciously turned off its AIS.[8]

Similarly, in August 2025, a fleet of seven Chinese RO-RO ferries, including the "Bo Hai Heng Da", sailed south from the Bohai Sea, gathered briefly in Quanzhou Bay, and then anchored in a designated military drill zone in the Red Bay area of Shanwei. This action perfectly aligned with a navigation warning issued by the Shanwei Maritime Safety Administration prohibiting civilian entry into the area due to military exercises.[9] These periodic, massive drills utilizing civilian RO-RO ferries, deck cargo ships, and even cruise ships demonstrate China's intent to normalize the rapid mobilization of civilian assets for potential amphibious assaults or blockade operations against Taiwan.

3. Exploiting the Depths: Unmanned Underwater Vehicles (UUVs)

China's gray-zone operations extend deep beneath the ocean surface. To gain underwater supremacy in the Western Pacific, China is heavily investing in Unmanned Underwater Vehicles (UUVs) and Long-Range Autonomous Underwater Vehicles (LRAUVs), such as the "Sea-Wing" and "Sea-Dolphin" gliders. These assets are frequently deployed under the guise of marine scientific research and exploration.[10]

These UUVs are crucial for "Battlespace Preparation". By carrying sensors that measure temperature, salinity, and depth across vast ocean areas, the Chinese military can calculate precise "sound speed profiles". This oceanographic intelligence allows their anti-submarine forces to identify "Acoustic Shadow Zones" where their own submarines can hide undetected, and map out "Convergence Zones" and "Bottom Bounce" areas to detect adversary submarines from much greater distances.[11]

---

8. MarineTraffic, "Ji Long Dao," accessed October 29, 2025, https://www.marinetraffic.com/en/ais/details/ships/shipid:6667360.
9. Lin Chuankai and Lin Chauluen, "China's Ro-Ro Ships' Potential Threats and Countermeasures: Taking 'Bohai Hengda' as an Example," *Defense Security Brief,* August 22, 2025, https://indsr.org.tw/focus?uid=11&pid=2891&typeid=34.
10. Wei Ren, Mo Li, and Yan-bo Gao, "Recent Developments in Underwater Gliders in China," *Marine Technology Society Journal* 54, No. 2, March/April 2020, https://www.ingentaconnect.com/contentone/mts/mtsj/2020/00000054/00000002/art00005.
11. The author's statement regarding the possible use of unmanned underwater vehicles by China is based on his nearly 34 years of naval service and his research on anti-submarine warfare and related background information.

Furthermore, these systems are transitioning from passive data collection to active anti-submarine warfare. The “Sea-Dolphin” glider, equipped with micro deep-sea piezoelectric vector sensors and built-in signal processors, can autonomously detect, track, and identify the acoustic signatures of advanced enemy submarines. Deployed in large numbers across the South China Sea, the Philippine Sea, or the Taiwan Strait, these low-cost, high-endurance gliders form a powerful underwater early warning line. In the future, driven by Artificial Intelligence, these UUV swarms could be equipped with explosive warheads or mine-countermeasure modules, acting as mobile minefields or conducting swarm attacks on high-value transport and surface combatant ships during the onset of a conflict.

4. Ghost Ships, AIS Spoofing, and Illicit Transfers

China’s gray-zone tactics also involve complex maritime deception, particularly the use of “Ghost Ships” and AIS spoofing to evade international regulation and sanctions. A notable case involved a vessel broadcasting the MMSI code 677058400 under the name “Eternal 1”. Investigations revealed that this ship was illegally using the identity of a 1973 general cargo ship named “AL MAJED H” (IMO number 7319694), a vessel that had officially been recorded as “Broken Up” (dismantled).[12]

This ghost ship displayed numerous anomalies: its registration details were blank, its insurance status was unknown, and it frequently swapped flags of convenience, including those of Tanzania, Panama, Vanuatu, and Cyprus. The ship’s AIS data was clearly manipulated; within minutes, it switched its IMO code between the dismantled ship’s number, another number (7116896), and “unknown”. Its destination constantly toggled between Busan, Taipei, Kaohsiung, and Hong Kong, while its reported draft wildly fluctuated between 0.5 meters and 4.5 meters.

Crucially, in March 2025, AIS tracking recorded this cargo ship physically mooring alongside a Chinese fishing vessel named “Liaoyingyu36099”.[13] This ship-to-ship transfer behavior is a strong indicator of illegal activities such as smuggling, unauthorized cargo trading, or espionage in sensitive geopolitical zones. Such ghost ships frequently roam the Exclusive Economic Zones (EEZ) of Taiwan and neighboring nations, exploiting legal gray areas.

12. “MarineTraffic Live Ships Map,” https://www.marinetraffic.com/en/ais/details/ships/shipid:734094.

13. “MarineTraffic Live Ships Map,” https://www.marinetraffic.com/en/ais/details/ships/shipid:10082618.

5. The Emergence of Private Armed Security Companies as Proxy Forces

A newly observed dimension in China's gray-zone strategy is the utilization of Private Military and Security Companies (PMSCs). Historically, Chinese private security firms did not carry weapons, but to protect expanding overseas interests, China has allowed the rise of armed private security firms.

In May 2026, a private security ship named "Hui Chuan", operated by the Chinese firm Sinoguards Marine Security and flying a Honduran flag, was seized by Iranian authorities near the Strait of Hormuz. Sinoguards is registered in Hong Kong, giving it a legitimate multinational corporate facade, but it operates as a vital tool in Beijing's overseas risk management architecture. The company hires foreign mercenaries—including veterans from Europe, Ukraine, and Nepal—equipped with heavy weapons like AK-47s to escort state-owned Chinese shipping fleets, such as those of COSCO Shipping.[14]

For Taiwan, the maturity of these Chinese armed PMSCs represents a new threat. In the event of an escalation in the Taiwan Strait, the PLA could easily repurpose these combat-experienced, heavily armed private security vessels as an upgraded proxy force or advanced maritime militia. Under the pretext of "protecting legitimate Chinese maritime interests", these vessels could harass Taiwanese forces, gather intelligence, or participate in a blockade, all while using their non-governmental status to bypass traditional military rules of engagement.

6. Escalation to Quasi-Military Actions: The Three-Tiered Structure

China's gray-zone tactics are not static; they are gradually escalating. A critical turning point occurred on August 11, 2025, near the Scarborough Shoal (Huangyan Island) in the South China Sea. During a high-speed pursuit of the Philippine Coast Guard patrol vessel "Suluan", a PLA Navy Type 052D destroyer ("Guilin") and a China Coast Guard (CCG) vessel ("3104") collided with each other. The CCG vessel suffered severe damage to its bow, resulting in casualties among the Chinese crew.[15]

---

14. Benoit Faucon and James T. Areddy, "Iran's Seizure of Chinese Security Ship Shows Its Favors for Friends Have Limits," *The Wall Street Journal*, May 16, 2026, https://www.wsj.com/world/china/irans-seizure-of-chinese-security-ship-shows-its-favors-for-friends-have-limits-f245618e?mod=hp_lead_pos5.
15. Captain James E. Fanell, "The Scarborough Shoal Incident: A '2.0' Plan Inches Closer to War," *Proceedings*, August 2025, https://www.usni.org/magazines/proceedings/2025/august/scarborough-shoal-incident-20-plan-inches-closer-war.

This incident exposed China's aggressive "Three-Tiered" maritime force structure: the maritime militia and civilian ships act as the first line of contact; the CCG serves as the second line; and the PLA Navy and Air Force act as the third line of deterrence. The collision was a direct result of the high-risk "high-speed encirclement" tactic and severe coordination failures between the Navy and the Coast Guard. The two branches operate under different command chains and communication protocols, leading to fatal misjudgments during complex joint operations. Shockingly, the commander of the "Guilin" did not stop to rescue the injured Coast Guard personnel, prioritizing top-down orders to intercept the Philippine ship over international maritime search and rescue obligations.

The direct involvement of a PLA Navy destroyer in a frontline interception signifies a dangerous escalation from "maritime law enforcement" to "quasi-military operations". By blurring the lines between military conflict and law enforcement, China creates strategic ambiguity, making it incredibly difficult for adversaries to determine the appropriate nature and intensity of their response.

II. COMPREHENSIVE COUNTERMEASURES

The integrity of the maritime domain and the survival of regional democracies hinge on a coordinated, transparent, and resolute response to these deceptive and persistent gray-zone tactics. Based on the detailed analysis of China's operational patterns, Taiwan and its allies must implement a comprehensive framework of countermeasures, heavily emphasizing technological superiority, clear rules of engagement, and international cooperation.

1. Information and Cognitive Warfare: Exposing the Shadows

The primary advantage of China's gray-zone strategy is its ambiguity. To defeat this, Taiwan must adopt a strategy of "radical transparency" to strip away the plausible deniability of the Chinese maritime militia and MCF vessels.

(1) Establish Comprehensive Databases: Taiwan's security agencies must systematically integrate intelligence to build a massive, real-time database of Chinese maritime militia and dual-use RO-RO ferries. This database must track ship names, ownership structures, historical movement patterns, and MCF exercise participation. By treating these supposedly civilian ships as military assets during peacetime tracking, Taiwan can accurately gauge the PLA's mobilization capabilities.

(2) Technological Superiority in Surveillance: Because Chinese militia ships

frequently turn off their AIS to operate as “dark vessels”, traditional monitoring is insufficient. Taiwan must leverage advanced space-based surveillance. Currently, Taiwan is partnering with two friendly foreign nations that provide satellite surveillance and reconnaissance capabilities through a confidential application, allowing Taiwan to track these dark vessels in real-time. Furthermore, Taiwan must accelerate the development of its own sovereign low-earth-orbit satellite monitoring capabilities to ensure independent, uninterrupted deterrence against gray-zone activities.

(3) Public Exposure and Multilingual Social Media Campaigns: Following the model of international think tanks like CSIS, Taiwan must regularly and publicly release concrete evidence (such as satellite imagery, drone footage, and intercepted communications) of China’s illicit activities. By rapidly exposing these actions on multilingual social media platforms, Taiwan can dominate the narrative, counter Chinese cognitive warfare, and impose massive reputational and political costs on Beijing, potentially forcing Chinese managing organizations to act with more caution.

2. Layered Defense and the Concept of “Existence Against Existence”

To counter China’s overwhelming numerical advantage and its three-tiered force structure, Taiwan must implement a highly disciplined, layered defense strategy.

(1) The Double-Layer Alert Line: Taiwan must strictly separate its law enforcement response from its military response to avoid falling into China's trap of escalating a civilian encounter into a military war. When facing gray-zone intrusions (such as a swarm of militia fishing boats or a CCG harassment operation), the Taiwan Coast Guard must always be deployed on the absolute front line to handle the situation under the legal framework of domestic law enforcement. Simultaneously, the Taiwan Navy must remain positioned in the rear as a standby deterrent and support force. This precise division of labor ensures that China cannot use Taiwan’s military presence as a pretext for a kinetic escalation.

(2) “Existence Against Existence”: Affected nations must maintain a constant, visible, and unyielding presence in their Exclusive Economic Zones. Recognizing the massive resource advantage of China’s layered deployment, Taiwan and neighboring democracies must adopt an “existence against existence” model. This means matching China’s physical presence on the water with Coast Guard patrols to assert legal jurisdiction and actively prevent Chinese vessels from operating arbitrarily or normalizing their encroachments.

3. Upgrading Rules of Engagement (ROE) and Asymmetric Capabilities

Frontline personnel face immense pressure when dealing with aggressive, quasi-military civilian vessels. The legal and tactical frameworks must be upgraded to support them.

(1) Clear and Specific ROE: Taiwan must continuously review and update its Rules of Engagement and emergency response protocols. The ROE must clearly define the exact conditions under which Coast Guard personnel can use warning shots, water cannons, or lethal force against heavily fortified militia ships (such as those armed with steel bars). Providing frontline personnel with unambiguous, risk-graded response options prevents both inadequate reactions that project weakness and excessive reactions that could trigger a war.

(2) Deploying Asymmetric Unmanned Systems: To counter the sheer volume of Chinese militia and UUVs, Taiwan must heavily invest in asymmetric, unmanned technologies. Deploying long-endurance Unmanned Aerial Vehicles (UAVs) and Unmanned Surface Vehicles (USVs) allows Taiwan to maintain continuous, wide-area surveillance and deterrence over gray-zone swarms without exposing expensive, manned naval vessels to the risks of ramming or attrition. These unmanned systems drastically reduce resource consumption and shorten decision-making times during high-stress encounters.

(3) AI-Driven Detection of Ghost Ships: To counter AIS spoofing and illegal ship-to-ship transfers, maritime and Coast Guard authorities must upgrade their Vessel Monitoring Systems (VMS). By integrating big data and artificial intelligence algorithms, these systems can automatically cross-reference broadcasting IMO codes against global registries in real-time. If a system detects a vessel transmitting the IMO of a “dismantled” or “sunken” ship, or exhibiting impossible draft changes, the system must instantly flag it. Taiwan must establish a “High-Risk Watchlist” (a Common Operational Picture) and mandate forced interception and boarding of vessels exhibiting these traits. If illegal, alterable AIS equipment is found, the vessel must be seized and its shipping agents prosecuted.

4. International Cooperation and Legal Warfare (Lawfare)

Gray-zone tactics exploit the seams in international law and boundaries. Therefore, the response must be deeply collaborative and legally grounded.

(1) Deepening Intelligence Sharing and Joint Patrols: Taiwan must actively construct real-time intelligence-sharing mechanisms with regional allies, including the United States, Japan, and the Philippines. When a problematic vessel, such as

an AIS-spoofing ghost ship or an armed private security vessel, is detected fleeing across maritime borders, this multinational network can enable rapid, coordinated interception and boarding. Furthermore, democratic nations should explore conducting joint patrols or maritime exercises at appropriate times to send a unified, powerful signal of deterrence to Beijing.

(2) Pushing International Lawfare: Taiwan and its allies must utilize international legal frameworks, primarily the United Nations Convention on the Law of the Sea (UNCLOS), to continuously challenge the legality of China's actions. States must issue strong diplomatic protests against unilateral actions, such as unauthorized oil exploration or the establishment of "natural reserves" in contested waters like the Scarborough Shoal, highlighting that these actions violate international law and threaten global energy and supply chain security. By forming a united front to condemn China's domestic laws (like its Coast Guard Law) that attempt to supersede international norms, the international community can solidify the rules-based maritime order.

5. Strengthening Domestic Defense Resilience

Finally, the ultimate target of gray-zone tactics is the psychological resolve of the target nation's population. Taiwan must build an impenetrable societal defense.

(1) Enhancing Public Defense Consensus: Taiwan must implement comprehensive public education campaigns to help citizens thoroughly understand the nature, intent, and limitations of China's gray-zone intrusions. By transparently communicating the realities of the threat, the government can inoculate the public against panic, psychological warfare, and the cognitive manipulation that China frequently attempts to spread through social media.

(2) Securing Critical Infrastructure: Gray-zone operations often serve as precursors to sabotage. Taiwan must drastically elevate the protection and redundancy of its critical infrastructure, particularly ports, power grids, and submarine communication cables. Ensuring that these facilities have robust backup systems and the capacity for rapid repair after an attack is absolutely essential to maintaining national security and societal functions during a prolonged crisis or a transition from gray-zone harassment to a full-scale blockade.

CONCLUSION

The PRC's gray-zone campaign is a highly sophisticated, multi-domain

strategy that leverages everything from deceptive fishing militia and dual-use RO-RO ferries to ghost ships, UUVs, and armed private security proxies. By operating below the threshold of war, China seeks to exhaust its neighbors and slowly alter the geopolitical reality of the Indo-Pacific. However, by deeply understanding these patterns, Taiwan and the democratic world can implement a formidable web of countermeasures. Through radical transparency, AI-enhanced surveillance, strict rules of engagement, layered “existence against existence” defense, and unyielding international legal cooperation, the international community can effectively neutralize the gray-zone threat and ensure long-term regional stability.

Drones, Demography, and Deterrence: Taiwan's Evolving Reserve Forces

*Dr. Harun Talha Ayanoglu**

I. INTRODUCTION

Taiwan maintains one of the largest reserve forces in the world, with close to two million individuals registered in its mobilization system, placing it among the top five globally alongside Vietnam, Ukraine, South Korea, and Russia.[1] However, numbers alone have not translated into strategic credibility. Persistent concerns over training cycles, equipment availability, and rapid mobilization capacity raise doubts about how much of this force could be effectively deployed in a high-intensity contingency. The gap between headline figures and actual readiness has therefore become a central issue in assessing Taiwan's defense posture.

Russia's full-scale invasion of Ukraine in 2022 reshaped how modern warfare is understood and influenced defense thinking in Taiwan. While much attention has been given to Ukraine's use of distributed operations and precision strikes, a more significant shift lies in how manpower has been used alongside unmanned systems. Ukrainian forces integrated mobilized personnel into decentralized drone operations, extending surveillance, targeting, and strike capabilities to the squad and even individual levels. This experience is particularly relevant for Taiwan, which by early 2026 has entered the category of a super-aged society with a shrinking pool of conscription-age citizens. Unlike Ukraine, Taiwan faces long-term demographic pressure that challenges manpower-intensive defense models.

---

* Harun Talha Ayanoglu holds PhD in Asia-Pacific Studies from National Chengchi University and is currently a Visiting Scholar at the Institute for National Defense and Security Research. His research focuses on nontraditional security threats and emerging technologies, with particular emphasis on unmanned weapon systems, military transformation, and their implications for contemporary conflicts and defense policy.

1. Global Firepower, "Reserve Military Manpower by Country (2026)," *Global Firepower,* 2026, https://www.globalfirepower.com/active-reserve-military-manpower.php.

In this context, Ukraine illustrates how limited human resources can be strengthened through technology in war time, while South Korea shows that similar adaptations can be introduced in peacetime through institutional changes in conscription and training. Taiwan's reserve force is therefore not only shaped by these developments but is increasingly moving in a similar direction, adapting its structure and training to align with the demands of a more technology-driven battlefield. This article argues that Taiwan's ability to sustain credible deterrence will depend not on the size of its reserve force alone, but on how effectively it integrates manpower with scalable and operationally relevant unmanned systems under conditions of demographic constraint.

II. UKRAINE AND THE TRANSFORMATION OF MODERN WARFARE

The use of drones in the Ukraine war represents a significant milestone, not only in terms of technological advancement but also how unmanned systems have been integrated into evolving combat concepts. In the early stages of the war, Ukraine relied heavily on foreign-manufactured drones as international support was at its peak. As the conflict shifted into a war of attrition, Ukraine began developing and fielding its own systems. Initially based on repurposed commercial platforms, these efforts evolved into domestically produced drones capable of fulfilling a wide range of operational roles, including intelligence, surveillance, and reconnaissance (ISR), precision strike, and deep strike missions.[2] Combined with a broader transition toward a distributed, flexible, and scalable defense approach, the widespread deployment of drones became central to battlefield operations. The integration of unmanned surface vessels (USVs) further enabled Ukrainian forces to sustain precision strike capabilities despite ammunition shortages.[3]

This operational shift was accompanied by a transformation in Ukraine's military-industrial model. Due to necessity, a decentralized and improvised production ecosystem emerged, in which civilians played active roles not only as operators but also as manufacturers. DIY drone production became a defining feature of Ukraine's wartime economy, with individuals converting garages,

2. "Ukraine's Civilians Play Key Role in Drone War," *NHK World*, 2024, https://www3.nhk.or.jp/nhkworld/en/news/backstories/3093/.

3. Kateryna Bondar, *Ukraine's Future Vision and Current Capabilities for Waging AI-Enabled Autonomous Warfare* (CSIS, 2025), 39, https://www.csis.org/analysis/ukraines-future-vision-and-current-capabilities-waging-ai-enabled-autonomous-warfare.

workshops, and former industrial facilities into small-scale production sites.[4] Civilian-led manufacturing blurred the traditional boundaries between military and civilian domains, demonstrating that large-scale mobilization does not have to rely on conventional structures. Instead, decentralized and technology-driven production networks enhanced resilience and sustained frontline capabilities.[5] In this context, civilians became embedded in national defense across a wide range of roles.

While civilian mobilization itself is not unique, Ukraine's integration of civilians as drone operators and contributors to a distributed production system marks a distinct development.[6] From the early stages of the war, mobilized personnel were increasingly assigned to drone-related roles as unmanned systems became dominant on the battlefield. Estimates suggest that approximately 60 percent of frontline strike capability and nearly 80 percent of casualties have been attributed to drone operations, underscoring their central role. To support this shift, Ukraine established drone training schools across the country, providing instruction to both civilians and reservists. Reports from these programs indicate that younger, tech-savvy individuals, particularly those with gaming experience, have been especially effective due to their familiarity with digital interfaces and control systems. Typically aged between 18 and 27, these individuals demonstrate strong hand-eye coordination and adaptability, while those with IT or engineering backgrounds often outperform others. Notably, even individuals with certain physical impairments have been successfully trained and deployed in drone operations.[7]

This transformation has been reinforced by continuous innovation in training and operational incentives. In 2025, Ukraine introduced the "Army of Drones Bonus System," a game-based reward mechanism that incentivizes operators based on confirmed strike outcomes. Personnel accumulate points for destroying equipment or inflicting casualties, which can then be exchanged for drone-related hardware through online stores. Between August and September alone, participating units increased from 95 to 400, with reported 18,000 Russian casualties linked to drone

4. Margaux Seigneur, "From Florist to Drone Maker: The Civilians Arming Ukraine's Drone War," *Inkstick,* 2026, https://inkstickmedia.com/from-florist-to-drone-maker-the-civilians-arming-ukraines-drone-war/.

5. NHK World, "Ukraine's Civilians Play Key Role in Drone War."

6. KC Cheng, "The FPV Drone Pilots Behind the Ukrainian War," *International Women's Media Foundation,* 2026, https://www.iwmf.org/reporting/the-fpv-drone-pilots-behind-the-ukrainian-war/.

7. Sinéad Baker, "Who Makes the Best Combat Drone Pilots? Ukrainian Drone Schools Say It's Young, Tech-Loving Gamers and People Used to Staring at Screens," *Business Insider,* 2025, https://www.businessinsider.com/ukraine-schools-say-best-drone-pilots-young-tech-loving-gamers-2025-12.

operations.[8] Moreover, Ukraine sought to expand access to training through the release of the Ukrainian Fight Drone Simulator (UFDS) on the Steam platform in late 2025. Developed using frontline feedback, the simulator replicates real combat conditions and has been used to train over 5,000 operators.[9]

Taken together, Ukraine's experience demonstrates that the significance of drones lies not merely in their tactical utility, but in their ability to reorganize the relationship between manpower, industry, and combat operations. Their relative affordability, scalability, and accessibility allow them to act as force multipliers in ways that do not depend on technological sophistication alone. At the same time, certain aspects remain context-specific, including the scale of wartime improvisation and the intensity of societal mobilization driven by existential threat. Nevertheless, the broader trajectory toward decentralized, technology-enabled combat supported by both military and civilian actors has begun to extend beyond the Ukrainian battlefield, shaping how other states approach the integration of manpower and emerging technologies in national defense.

III. SOUTH KOREA: INSTITUTIONALIZING DRONE-ENABLED CONSCRIPTION

The year 2022 marked a turning point in South Korea's reassessment of unmanned systems in national defense. A series of North Korean drone incursions into South Korean airspace exposed critical gaps in surveillance and response capabilities, highlighting vulnerabilities in counter-UAV preparedness. In response, Seoul accelerated efforts to develop and deploy unmanned systems to monitor and deter North Korean activities. At the same time, the war in Ukraine demonstrated the growing centrality of drone-saturated, asymmetric combat concepts, where unmanned systems were not only force multipliers but integral components of operational design. Observing these developments, South Korea moved to incorporate similar principles into its defense planning. This shift extended beyond platform acquisition, aiming to embed drone capabilities within both active forces

8. Robert Booth, "Ukrainian Computer Game-Style Drone Attack System Goes 'Viral'," *The Guardian*, 2025, https://www.theguardian.com/world/2025/nov/03/ukrainian-computer-game-style-drone-attack-system-goes-viral.

9. Johanna Urbancik, "Drone Combat at Home: Simulator Lets Players Step into the Frontline," *Euro News,* 2025, https://www.euronews.com/2025/12/10/drone-combat-at-home-simulator-lets-players-step-into-the-frontline.

and the broader conscription system.

Based on these, in late 2025 Korea announced the “500,000 Drone Warriors” initiative, to be implemented from 2026 onward. The initiative seeks to enhance combat readiness by training all conscripts in drone operations while increasing civilian familiarity with unmanned systems. To support this effort, the Ministry of National Defense allocated approximately USD 22.9 million for the procurement of 11,184 small commercial drones for training. Currently, the armed forces operate around 1,100 training drones; with this expansion, the number of platforms will increase substantially, enabling each army squad to be equipped with at least one drone. This scaling effort reflects an intention to normalize drone usage at the lowest tactical levels.[10]

The doctrinal implications of this initiative have been explicitly acknowledged by Korean defense leadership. The Minister of National Defense described drones as a “second personal weapon,” signaling a shift treating drone proficiency not as a specialized skill but as a baseline capability for conscripts. Despite implementation challenges, the initiative represents a notable attempt to align conscription and reserve structures with the requirements of technology-intensive warfare.[11] More broadly, Seoul’s approach illustrates how lessons observed in Ukraine can be translated into peacetime force development. By institutionalizing drone training within conscription, Seoul is not only enhancing immediate military readiness but also cultivating a broader base of personnel familiar with unmanned systems before the onset of crisis. This experience provides a useful point of comparison for Taiwan, where similar pressures to adapt reserve and conscription structures are emerging under different structural constraints.

IV. TAIWAN’S RESERVE FORCES UNDER PRESSURE

1. Demographic Constraint

Population aging has long posed structural challenges to Taiwan’s social and economic sustainability, but by early 2026 it has acquired direct strategic

10. https://www.mnd.go.kr/user/boardList.action?command=view&page=1&boardId=O_47261&boardSeq=O_400324&mcategoryId=&id=mndEN_020100000000.

11. Joon Ha Park, “South Korea’s Drone Warrior Plan Faces Hurdles beyond Training and Hardware,” *Korea Pro*, 2025, https://koreapro.org/2025/09/south-koreas-drone-warrior-plan-faces-hurdles-beyond-training-and-hardware/.

significance. Data from the Ministry of the Interior confirms that Taiwan has entered the category of a "super-aged" society, with more than 20 percent of its population over 65.[12] With one of the world's lowest fertility rates and a steadily shrinking population, the island faces long-term and largely irreversible pressures. While aging is common among advanced economies, Taiwan's geopolitical environment makes this trend particularly consequential. Declining birth rates are narrowing the pool of conscription-age citizens, increasing strain on manpower planning for national defense. Despite maintaining a large mobilization base on paper, projections suggest that sustaining a manpower-intensive reserve system will become progressively more difficult over the medium to long term. Under these conditions, Taiwan's demographic trajectory is not only a socioeconomic issue but a strategic constraint that challenges the long-term viability of Taiwan's existing defense model.

2. Reserve Structure Problems

Taiwan's transition to an all-volunteer force (AVF), formalized in 2019 with the reduction of conscription to four months, was intended to reduce social and economic costs while building a smaller, more professional, and technologically advanced military. However, this transformation introduced new challenges. Despite professionalization efforts, concerns persisted regarding combat readiness, as the system often prioritized recruitment targets over training quality and operational capability. At the same time, demographic decline further constrained the pool of potential volunteers and conscripts, exacerbating manpower shortages.[13]

In response to the Ukraine War and rising cross-Strait tensions, Taiwan reinstated one-year conscription beginning in 2024, acknowledging the limitations of the previous system.[14] Nevertheless, structural constraints remain. Aging demographics continue to pressure on both annual conscription levels and long-term mobilization capacity. To mitigate this, the Ministry of National Defense (MND) has sought to expand the eligible manpower pool by revising conscription standards. By the end of 2025, proposed amendments to the Physique Classification Standards

12. Ministry of Interior, ROC, "Monthly Bulletin," *Ministry of Interior, Republic of China (Taiwan)*, 2026, https://www.moi.gov.tw/english/cl.aspx?n=7665.

13. Vanessa Molter, "Taiwan's Transition to an All-Volunteer Force — A Policy Assessment and Recommendations," *Defense Security Brief* (Taipei, Taiwan), 2019.

14. Richard Heraud, "Military Education and the New 12-Month Conscription Program: An Imperative, Not a Choice," *Defense Security Brief* (Taipei, Taiwan), 2024.

of Military Service updated 80 out of 193 medical criteria, narrowing eligibility for exemptions and aiming to reduce an exemption rate of around 16 percent, which is high by international standards. This reflects growing concern over the sustainability of Taiwan's manpower base.[15]

These constraints are also evident in the reserve force structure, where headline figures obscure limited readiness. While nearly two million reservists are formally registered, only around 700,000 fall within the category eligible for periodic training, and in practice, roughly 100,000 to 110,000 receive annual training.[16] As a result, only a small fraction of the mobilization pool is actively trained in any given year. Training duration remains uneven, with some reservists receiving as little as five to seven days, while others participate in slightly extended but still limited programs. Budgetary constraints, limited training facilities, and shortages of qualified instructors further restrict the system's ability to expand training coverage. Consequently, despite its large numerical base, Taiwan's reserve force remains only partially prepared, and the number of personnel that could be rapidly mobilized, equipped, and deployed in a high-intensity conflict remains uncertain.

3. Credibility Issue

The effectiveness of deterrence depends not on capabilities themselves, but on how capabilities are perceived by a potential adversary. In this regard, Taiwan's reserve forces appear to carry limited weight in Chinese strategic assessments. Chinese military analyses from early 2000s acknowledged that Taiwan's reservists could complicate amphibious operations, particularly in urban and mountainous terrain where terrain favors the defender. At the same time, these assessments consistently highlighted structural weaknesses, including shortened conscription periods, limited training, and resource constraints.[17]

More recent official discourse suggests even less emphasis on Taiwan's reserves. High-level analyses tend to focus on six primary areas: Taiwan's political leadership, defense strategy, military exercises, arms acquisitions, foreign military cooperation, and internal issues affecting morale. Within this framework, reserve

15.〈國防部公告：預告「體位區分標準」修正草案〉，《公共政策線上參與平臺》，2025 年 12 月 12 日，https://join.gov.tw/policies/detail/b6804583-7dd9-4206-afb6-43b9f465ca27。

16.〈立院報告：列管後備軍人逾 6 成未曾召訓 不利戰力提升〉，《中央社》（*Central News Agency*），2024 年 11 月 3 日， https://www.cna.com.tw/news/aipl/202411030056.aspx。

17. David G. Brown, "Reconceiving Taiwan's Reserve Forces," *Defense Security Brief* (Taipei, Taiwan), 2020.

forces are rarely treated as a decisive factor, even in discussions of mobilization and manpower.[18] This relative absence indicates that, at the strategic level, Taiwan's reserve force does not significantly influence Chinese operational planning. In effect, while large in numerical terms, the reserve system contributes little to deterrence if it is not perceived as a credible and operationally relevant capability.

V. TAIWAN'S ONGOING ADAPTATION: DRONE INTEGRATION AND TRANSFORMATION

Following the lessons observed in the Ukraine war, Taiwan's MND and Reserve Force Command have begun to reassess the role of unmanned systems within national defense. This shift extends beyond the military domain and reflects a broader understanding that effective drone development requires interagency coordination across sectors such as law enforcement, emergency response, agriculture, and civilian technology industries. In this sense, drones are increasingly viewed not only as military assets but as components of a broader national capability. At the same time, Taiwan's strong technological base positions it well for advanced drone development. However, recent conflicts suggest that effectiveness in drone warfare does not necessarily depend on technological sophistication alone. Experiences from Ukraine and other contemporary battlefields indicate that relatively simple, low-cost, and scalable systems, when integrated into a coherent operational doctrine, can impose significant costs on adversaries and complicate their defenses. This raises the question of whether technological advancement alone is sufficient, or whether greater emphasis should be placed on scalability, deployment, and doctrinal integration.

At the same time, Taiwan's conscription system has undergone parallel adjustments in response to the evolving security environment. In 2024, compulsory military service was extended from four months back to twelve months, reflecting concerns over combat readiness and the limitations of the previous all-volunteer force model. Under the current system, individuals enter the reserve force for eight years after service and are called for refresher training every two years, typically lasting fourteen days. Discussions within the armed forces indicate further reform considerations. According to former Reserve Command head, retired General Pai

18. Ian Easton et al., "Transformation of Taiwan's Reserve Force," *RAND Corporation*, 2017, p. 85, https://www.rand.org/pubs/research_reports/RR1757.html.

Chieh-lung, there is a long-term vision of restructuring the system toward a four-year reserve cycle with fourteen days of annual refresher training. While not yet implemented, such proposals indicate an effort to maintain a more consistently trained force. However, institutional change remains gradual, shaped by constraints in planning, budgeting, and personnel allocation. Previous adjustments, such as extending refresher training from five to fourteen days, required five years to implement, suggesting that transformation within the reserve system is incremental rather than immediate.

Within this broader reform trajectory, drone integration has emerged as a notable development. Beginning in 2025, Taiwan introduced drone training into its conscription program. According to the Executive Yuan's 2025 Policy Address and subsequent implementation updates from the MND in 2026, this training is structured in two phases. The first phase provides basic knowledge, including flight principles, legal regulations, simulator familiarization, and introductory operation of drones produced by the National Chung-Shan Institute of Science and Technology (NCSIST). The second phase involves more advanced, unit-level training, including field exercises and specialized FPV training. Rather than applying a uniform model, the MND employs skill-matching to align training with conscripts' civilian expertise, particularly in technical fields. Although current training remains limited in duration, there are indications that more advanced modules may be expanded.

In operational terms, the integration of drones into Taiwan's force structure is most relevant when viewed against the island's specific defense requirements and structural constraints. Given limited manpower and the need for dispersed operations, unmanned systems can enhance the effectiveness of both active and reserve forces in missions such as ISR in the littoral environment, as well as monitoring potential amphibious movements across the Taiwan Strait. They can also provide real-time targeting support for coastal defense and artillery units, improving precision without requiring large force concentrations. For reserve units, which may be mobilized under time and training constraints, drones offer a means to extend situational awareness in urban and complex terrain, as well as to detect and track airborne or heliborne insertion forces. In this sense, unmanned systems do not simply add new capabilities but help compensate for structural limitations by enabling smaller and less continuously trained units to operate more effectively within a distributed defense framework.

Reflecting this operational logic, drone integration has also been extended to reserve forces. Since October 2025, drone operations have been incorporated into the standard refresher training cycle, supported by the procurement of approximately

850 small drones distributed across reserve brigades, averaging 50 to 60 units per brigade. Training currently focuses on surveillance, reconnaissance, and artillery adjustment missions, while more complex systems remain restricted to specialized personnel.[19] At the same time, this integration has been partially linked to civilian skill development. Conscripts and reservists who demonstrate proficiency may receive training certifications that support applications for a "Remote Controlled Unmanned Aerial Vehicle Operator's License" issued by the Civil Aeronautics Administration, creating overlap between military training and civilian employment pathways.

Taken together, these developments suggest that Taiwan's reserve force is undergoing gradual adaptation rather than remaining static. However, the direction and depth of this transformation remain uneven. While Taiwan possesses strong technological capabilities, the experience of recent conflicts indicates that the effectiveness of unmanned systems depends less on technological sophistication than on how they are integrated into operational doctrine, scaled across units, and aligned with specific defense requirements. In this regard, Taiwan's ongoing efforts can be understood as an initial phase of adjustment, in which institutional reforms, training practices, and technological development are gradually converging. The extent to which these elements can be coherently integrated will play a decisive role in determining whether drone-enabled capabilities can meaningfully enhance the credibility and effectiveness of Taiwan's reserve forces.

VI. CONCLUSION

Taiwan's reserve force, long characterized by its numerical scale, is increasingly defined by the constraints and transformations outlined throughout this analysis. The Ukraine War has demonstrated that modern defense depends not only on manpower size, but on how that manpower is integrated with emerging technologies. Ukraine's experience showed that drones can reshape the relationship between personnel, firepower, and situational awareness, enabling decentralized and scalable combat. South Korea further illustrates that such transformations can be institutionalized in peacetime by embedding drone training within conscription systems to enhance both military readiness and societal familiarity with new technologies.

19. 〈58砲指部沉浸式無人機訓練　強化不對稱作戰能量〉，《軍聞社》（Military News Agency），2026年3月3日，https://mna.mnd.gov.tw/news/detail/?UserKey=d966ae83-f39a-4032-a545-55ecd9e4d883。

In Taiwan's case, these developments intersect with internal structural pressures, particularly demographic decline and a contracting mobilization pool. As the island becomes a super-aged society, the sustainability of a manpower-intensive reserve model becomes increasingly uncertain. Taiwan has begun to respond through the reintroduction of one-year conscription, adjustments in reserve training, and the integration of drone training into both conscription and refresher programs. While still limited in scope, these efforts indicate that the reserve force is evolving rather than remaining static.

At the same time, Taiwan's experience highlights that the effectiveness of this transformation will depend not simply on the adoption of new technologies, but on how these technologies are aligned with operational requirements and structural constraints. Recent conflicts suggest that relatively simple, scalable, and widely deployable unmanned systems can generate significant operational effects when integrated into a coherent defense framework. In this context, the strategic value of Taiwan's reserve forces will increasingly depend on their ability to leverage such systems to compensate for limitations in manpower, training depth, and mobilization speed.

In conclusion, the cases examined in this article suggest that the future effectiveness of reserve forces will depend less on numerical size and more on adaptability, scalability, and the integration of manpower with appropriately applied technology. For Taiwan, this implies that the ongoing transformation of its reserve system should be understood not as a discrete reform, but as part of a broader adjustment to the realities of contemporary warfare, where the credibility of defense rests on the effective combination of human resources, operational doctrine, and accessible technological capabilities.

Digital Resilience: Ukraine's Experience during the Russian-Ukrainian war and Its Implications for Taiwan

*Minchen Tseng**

I. INTRODUCTION

Since the outset of Russia's full-scale invasion in February 2022, Ukraine has faced systematic attacks on its digital and telecommunications infrastructure. According to Ukraine's Deputy Prime Minister and Minister of Digital Transformation, Mykhailo Fedorov, approximately 25% of fixed-line networks have been damaged, more than 4,300 mobile base stations have been destroyed or impaired, and over 30,000 kilometers of fiber-optic cables have been affected by kinetic strikes.[1] In response, Ukraine adopted a hybrid telecommunications and digital governance strategy that redefined digital resilience as a core pillar of national survival in high-intensity warfare. Ukraine's experience demonstrates that in contemporary conflict, the ability to sustain connectivity, preserve governance continuity, and defend the information environment can be as decisive as conventional military power. These lessons are particularly noticeable for Taiwan, which faces persistent gray-zone pressure, cognitive warfare, and the risk of infrastructure disruption. By examining Ukraine's digital resilience during wartime, this article seeks to identify transferable lessons and strategic adaptations that can inform Taiwan's efforts to strengthen its own digital resilience across connectivity, governance, and the cognitive domain.

---

* Ms. Minchen Tseng is a Policy Analyst at Division of Cyber Security and Decision-Making Simulation, INDSR. Her research interests include Digital Resilience, Cognitive Warfare, and Digital Authoritarian.

1. "В Україні пошкоджено чверть мереж фіксованого зв'язку і понад 4 тис. базових станцій мобільного зв'язку - Федоров," 〔In Ukraine, A Quarter of Fixed-line Networks and More Than 4,000 Mobile Base Stations have been Damaged — Fedorov〕 *Інтерфакс-Україна*, May 15, 2024, https://interfax.com.ua/news/telecom/986919.html.

II. UKRAINE'S DIGITAL RESILIENCE

1. Ensuring Connectivity under Fire

IT and telecom personnel reservation: The Ministry of Digital Transformation gained authority around September 2022 to shield critical IT and telecom workers from military conscription, recognizing their specialized skills vital for digital infrastructure resilience during wartime.[2] This policy aims to retain essential tech talent, ensuring communication networks and digital services remain functional despite ongoing conflict.

Public connectivity measures: Since November 2022, the Ukrainian government has rolled out a nationwide network of "Points of Invincibility"—public hubs equipped with electricity, free Wi-Fi, device charging, and satellite broadband[3]—which by 2023 had expanded to over 13,000 locations, providing civilians with guaranteed minimum digital connectivity and social stability during prolonged blackouts and repeated attacks on critical infrastructure.[4]

Redundancy and mandated service: Through regulatory coordination and industry consensus, Ukrainian mobile operators abolished domestic roaming fees and implemented emergency infrastructure-sharing arrangements, enabling subscribers to automatically connect to alternative networks when their home operator's base stations were damaged or destroyed,[5] thereby transforming commercial competition into a de facto national roaming regime that significantly strengthened continuity of connectivity during sustained attacks on telecom infrastructure.

Infrastructure protection: The Ministry of Digital Transformation has revised national reconstruction standards to systematically prioritize underground deployment of electronic communications networks, reducing exposure to air and

---

2. "Деякі питання реалізації положень Закону України "Про мобілізаційну підготовку та мобілізацію," щодо бронювання військовозобов'язаних на період мобілізації та на воєнний час," 〔Some Issues of Implementing the Provisions of the Law of Ukraine 'On Mobilization Preparation and Mobilization' Regarding the Reservation of Persons Liable for Military Service for the Period of Mobilization and Wartime〕 *Верховна Рада України*, January 27, 2023, https://zakon.rada.gov.ua/laws/main/76-2023-%D0%BF.
3. Kateryna Zarembo, Michèle Knodt and Jannis Kachel, "Smartphone Resilience: ICT in Ukrainian Civic Response to the Russian Full-scale Invasion," *Media, War & Conflict*, Vol. 18, No. 2, March 2024, p. 12.
4. Anhelina Sheremet, "More than 13 000 Points of Invincibility Have Already Been Deployed in Ukraine. You can Find Them in "Diia" App," *Babel.UA*, October 17, 2023, https://babel.ua/en/news/99653-more-than-13-000-points-of-invincibility-have-already-been-deployed-in-ukraine-you-can-find-them-in-diia-app.
5. "Ministry of Digital Transformation: Ukrainian Mobile Operators Will Allow Subscribers to Switch to the Network of Other Operators to Stay Connected," *GOV. UA*, March 7, 2022, https://pse.is/8hhbzr.

artillery strikes, improving survivability under repeated attacks,[6] and embedding physical resilience into Ukraine's long-term postwar digital infrastructure rather than treating protection as a temporary wartime measure.

Power support: The largest Ukrainian telecom provider—Kyivstar has made large-scale investments in power resilience by deploying thousands of backup generators and nearly 200,000 batteries across its facilities, ensuring that core network nodes can continue operating during prolonged blackouts and thereby sustaining nationwide communications even amid sustained attacks on the power grid.[7]

Rapid satellite & operator response: During the war's first two days, Ukraine's Deputy Prime Minister Mykhailo Fedorov sought help from Elon Musk, enabling Starlink to become the backbone of Ukraine's communications.[8] Local operators—Kyivstar, Vodafone Ukraine, and Ukrtelecom—restored connectivity where infrastructure was damaged. Vodafone Ukraine used Starlink terminals to quickly reconnect 2G/4G services near Irpin and Romanivka,[9] while Kyivstar employed "Direct to Cell" satellite links and movable base stations to maintain SMS（Short Message Service）and data.[10] Ukrtelecom repaired fiber to restore high-speed services in liberated areas.[11]

2. Maintaining Governmental and Societal Functionality

Diia and its ecosystem

Launched in 2020, Diia is Ukraine's comprehensive digital governance platform, integrating digital identity verification, access to official documents, taxation services,

---

6. Yuriy Matsyk, "Ukraine's Digital Resilience," *FiCom*, August 14, 2024, https://ficom.fi/news/ukraines-digital-resilience/.
7. "Internet and Mobile Communication During Blackouts: Kyivstar has Found a Solution," *Komersant Ukrainian*, January 15, 2025, https://komersant.ua/en/internet-ta-mobilnyy-zv-iazok-pid-chas-blekautiv-u-kyivstar-znayshly-rishennia/.
8. David Walsh, "Elon Musk Deploys SpaceX's Starlink Internet Satellites over Ukraine After Request from Vice PM," *Euronews*, February 27, 2022, https://www.euronews.com/next/2022/02/27/elon-musk-deploys-spacex-s-starlink-internet-satellites-over-ukraine-after-request-from-vi.
9. "Vodafone Ukraine Restores Communication in Settlements of Bucha District," *Interfax*, April 7, 2022, https://en.interfax.com.ua/news/general/821986.html.
10. Stefanie Schappert, "Ukrainians First to Get Starlink "Direct to Cell" Satellite Service in Europe," *Cybernews,* November 24, 2025, https://cybernews.com/news/starlink-kyivstar-launch-first-satellite-direct-to-cell-service-ukraine/.
11. "Ukrtelecom Gradually Resumes Operations in the Liberated Areas by Connecting Subscribers to Optic Fibre," *SCM*, May 1, 2023, https://scm.com.ua/en/news/ukrtelekom-postupove-vidnovlennya-roboti-na-zvilnenih-teritoriyah-ta-pidklyuchennya-do-optiki.

and interfaces with online banking systems. Over time, Diia has evolved beyond a single application into a broader digital governance ecosystem that reflects a new philosophy of statecraft.[12] This ecosystem includes Diia.Business, which supports entrepreneurs through grants and expert advisory services; Diia.Education, a nationwide digital literacy initiative that has reached more than 2.6 million Ukrainians; Diia.City, a specialized legal and tax framework designed to support over 1,700 IT companies; and Diia.Engine, an open-source low-code platform enabling government agencies to rapidly develop and deploy digital public services.[13]

Following Russia's full-scale invasion of Ukraine in 2022, many observers anticipated the collapse of Ukrainian government systems. Instead, the country's digital infrastructure not only withstood the initial shock but expanded in real time. The Ministry of Digital Transformation rapidly shifted Diia from a peacetime convenience into a core instrument of wartime governance and national resilience. Within days and weeks of the invasion, new digital services were launched, including eAssistance, which delivered financial support to millions of internally displaced persons; eVorog, which enabled secure civilian reporting of enemy movements; eRecovery, which streamlined housing repair assistance and property damage claims; and eMarriage, allowing couples to marry remotely despite wartime disruptions.[14]

Despite sustained missile strikes, air-raid alerts, power outages, cyberattacks, and mass displacement, Diia has remained operational—continuing to deliver essential public services, safeguard civil rights, and facilitate civic participation. By 2025, the platform had grown to serve more than 22.9 million users, offering over 150 services via its web portal, 65+ mobile services, 33 digital documents, and a public–private ecosystem comprising more than 25,000 partners.[15] In the context of the Russian-Ukrainian War, Diia has emerged as a critical digital lifeline linking the state and society, ensuring the continuity of governance under wartime conditions. More recently, the platform has further evolved into Diia.AI,[16] incorporating artificial

12. "Ukraine Digital Development Country Profile," *ITU*, May 2025, pp. 48-51.

13. George Ingram and Priya Vora, "Ukraine Digital Resilience in a Time of War Working Paper #185," *Center for Sustainable Development at Brookings,* January 2024, pp. 24-26.

14. Valeriya Ionan, "Ukraine's Digital Transformation as Europe's Digital Opportunity," *GovTech Intelligence Hub*, May 14, 2025, https://www.govtechintelhub.org/case-study-details/ukraine's-digital-transformation-as-europe's-digital-opportunity/aJYTG0000000ZXF4A2.

15. "Diia: From the Mobile App to the Digital State," *Apolitical,* September 18, 2025, https://apolitical.co/solution-articles/en/diia-from-the-mobile-app-to-the-digital-state-663.

16. Mykhailo Fedorov, "Diia.AI: The World's First National AI-Agent That Delivers Real Government Services," *Digital State UA*, September 3, 2025, https://digitalstate.gov.ua/news/govtech/diiaai-pershyy-u-sviti-derzavnyy-ai-ahent-iakyy-ne-prosto-konsultuye-a-nadaye-posluhy-iak-pratsiuye-shtuchnyy-intelekt-na-portali.

intelligence to enhance administrative efficiency, transparency, and the resilience of state–society interaction.

External Enablement: AWS & Microsoft

To ensure wartime continuity, AWS（Amazon Web Services）and the Ukrainian government executed an emergency high-speed migration, shifting critical data from vulnerable on-premises centers to the cloud. This unprecedented "digital evacuation" yielded significant results: 50 government authorities successfully migrated to AWS, protecting over 15PB of Ukrainian citizen data. Furthermore, 28 Ukrainian universities moved their operations to the cloud to preserve the nation's academic infrastructure.[17] On the other hand, Microsoft played an indispensable strategic role in constructing Ukraine's digital resilience. Its contributions extended beyond mere technical support, serving as a critical pillar for maintaining government stability and cybersecurity. Local Microsoft experts provided state-of-the-art technical tools that significantly reduced the time required to export sensitive state registers and operational data.[18] By providing access to advanced cloud computing resources and productivity suites, Microsoft ensured seamless cross-departmental communication, which was vital for efficient decision-making during wartime. These metrics suggest that Ukraine's resilience was not merely a result of pre-designed architecture, but rather a decisive, real-time intervention by external tech partners that saved an entire nation from digital destruction.

Reserve+ & Army+

In wartime conditions, traditional administrative and mobilization systems—reliant on paperwork, in-person processing, and fragmented information flows—are incapable of supporting large-scale, time-sensitive mobilization. To address this gap, Ukraine launched Reserve+ in 2024 to digitally integrate millions of citizens into the military manpower system. The platform enables electronic military registration, verification of military specialties, and profession-based unit assignment,[19] significantly enhancing the efficiency, accuracy, and transparency of conscription.

17. Kaido Einama, "The Cloud Saved a Nation: How Ukraine Backed Up an Entire Country During the War," *The Baltic Sentinel*, October 26, 2025, https://balticsentinel.eu/8350030/the-cloud-saved-a-nation-how-ukraine-backed-up-an-entire-country-during-the-war.
18. "How technology helped Ukraine resist during wartime," *Microsoft,* January 20, 2023, https://news.microsoft.com/en-cee/2023/01/20/how-technology-helped-ukraine-resist-during-wartime/.
19. "Ministry of Defence Launches Reserve+ Mobile Application," *Ministry of Defence of Ukraine*, May 17, 2024, https://mod.gov.ua/en/news/ministry-of-defence-launches-reserve-mobile-application-1.

In parallel, Army+ was developed as a digital personnel management platform for active-duty soldiers, replacing cumbersome paper-based procedures. Through Army+, soldiers can apply for leave, submit logistical and welfare requests, request position transfers, participate in surveys, access integrated commercial benefits, and strengthen training and professional skills.[20] Together, Reserve+ and Army+ function as critical digital enablers of wartime mobilization and force sustainment, allowing Ukraine to rapidly scale manpower, maintain organizational cohesion, and preserve operational effectiveness under prolonged high-intensity conflict.

3. Countering Disinformation and Information Warfare

United News

To secure the domestic information front, President Zelenskyy consolidated Ukraine's media landscape into a single, 24-hour broadcast platform shortly after the war began. Citing the necessity of a unified message under martial law, the government launched "Yedyni Novyny" (United News). This unprecedented "TV marathon" included 1+1 Media, StarLightMedia, and Inter Media Group which joined forces to co-produce a continuous news stream. By August 2022, nine of the nation's leading channels had integrated into this collective broadcast,effectively centralizing wartime communications.

Multi-layered fact-checking ecosystem

Layer 1: The State (Strategic Defense)

Institutions such as the National Security and Defense Council (NSDC), through its Center for Countering Disinformation (CCD), focus on identifying and countering high-level information threats that endanger national security, while the Ministry of Culture and Information Policy's StratCom Centre manages daily official communication and public myth-busting.[23] Complementing these reactive measures,

---

20. "Zelenskyy: "Army+" Application will be Available from Today," *UNN*, August 8, 2024, https://unn.ua/en/news/zelenskyy-army-application-will-be-available-from-today.
21. "Citing Martial Law, Ukraine President Signs Decree to Combine National TV Channels into One Platform," *Reuters*, March 20, 2022, https://www.reuters.com/world/europe/citing-martial-law-ukraine-president-signs-decree-combine-national-tv-channels-2022-03-20/.
22. Anastasiia Lapatina, "A Power Grab or a Weapon Against Russia? Ukraine's 'TV Marathon' Explained," *The Kyiv Independent,* September 27, 2023, https://kyivindependent.com/a-power-grab-or-a-weapon-against-russia-ukraines-tv-marathon-explained/.
23. Katong Ragawi Numadi, "Ukraine's Counter-Strategic Responses Toward Russian Propaganda and Disinformation During the War," *Jurnal Hubungan Internasional,* Vol. 18 No. 1, June 2025, p. 152.

long-term resilience is reinforced through educational initiatives such as National Media Literacy project "Filter",[24] which aims to improve media literacy and reduce societal vulnerability to hostile influence operations.

Layer 2: Civil Society (The Rapid Response Force)

Civil society organizations form the frontline of Ukraine's counter-disinformation ecosystem by providing rapid, decentralized responses to emerging falsehoods. Independent fact-checking NGOs, including StopFake and VoxCheck, act as first responders by verifying viral content using transparent methodologies, while media watchdogs such as Detector Media monitor broader narrative shifts and identify coordinated influence networks.[25] Crowdsourced verification initiatives, exemplified by Gwara Media's Telegram-based reporting tools,[26] further enhance responsiveness by enabling citizens to flag suspicious information for expert review in near real time.

Layer 3: Technical & OSINT (The Evidence Layer)

The technical and OSINT layer underpins the entire system by supplying verifiable, evidence-based refutations of disinformation. Groups such as InformNapalm and Molfar employ open-source intelligence techniques[27]—ranging from satellite imagery and geolocation to facial recognition and digital forensics—to produce highly credible, difficult-to-dispute proof. This layer is reinforced through direct cooperation with major technology platforms, including Meta (Facebook and Instagram), Twitter, LinkedIn, YouTube, Telegram which helps prioritize verified Ukrainian sources and disrupt coordinated inauthentic behavior,[28] thereby translating technical findings into tangible enforcement and visibility outcomes.

---

24. "'Filter' National Media Literacy Project Holds First Strategic Session," *UNDP*, June 20, 2023, https://www.undp.org/ukraine/press-releases/filter-national-media-literacy-project-holds-first-strategic-session.
25. "Ukraine's Media Landscape in 2022: Martial Law Unavoidably Restricted Freedom of Expression and Telegram Emerged as the Primary News Source Amidst War," *Centre for Media Pluralism and Media Freedom,* January 11, 2024, https://cmpf.eui.eu/ukranian-media-landscape-in-2022/.
26. "Fact-checking," *Gwara Media*, https://gwaramedia.com/en/factcheck/.
27. Olga Boichak and Andrew Hoskins, "My War: Participation in Warfare," *Digital War,* Vol. 3, No. 2, December 2022, p. 5.
28. "Regarding the Creation of a Unified Position ("One Voice") of Ukraine to Global Tech Platforms to Fight against Disinformation and Fakes," *SPRAVDI,* July 19, 2022, https://spravdi.org/en/regarding-the-creation-of-a-unified-position-one-voice-of-ukraine-to-global-tech-platforms-to-fight-against-disinformation-and-fakes/.

III. IMPLICATIONS FOR TAIWAN: STRATEGIC ADAPTATION FRAMEWORK

1. Strengthening Multi-Layered Connectivity Resilience

Ukraine's wartime experience demonstrates that connectivity resilience depends on early institutional adaptation, layered infrastructure redundancy, and rapid public–private coordination, showing that maintaining communications is as much about governance and planning as it is about technology. For Taiwan, the structural vulnerability of island geography is most evident in its dependence on submarine cable choke points. In recent years, China's interference with Taiwan's undersea cables has become increasingly systematic, combining gray-zone operations, technical sophistication, and plausible deniability. These actions fall short of open conflict yet aim to erode confidence, disrupt daily life, and test Taiwan's response thresholds. To mitigate these risks, Taiwan must transition toward a hybrid connectivity architecture that integrates:

- Submarine cables as the primary high-capacity backbone;
- Microwave links for short- to mid-range terrestrial and cross-island redundancy;
- Geostationary and Low Earth orbit (LEO) satellite systems to ensure continuity during large-scale outages or maritime disruptions;
- Portable and rapidly deployable backup stations, pre-positioned across the island to support critical infrastructure, government operations, and emergency services.

Crucially, resilience is not purely technological; Ukraine's experience highlights the importance of operational readiness and societal adaptation. Taiwan should institutionalize routine, peacetime connectivity drills across critical infrastructure operators, local governments, hospitals, financial institutions, and key industries to stress-test technical capabilities, refine public–private coordination, and reduce public panic by normalizing contingency procedures. Integrating these exercises into daily governance and business continuity planning would make resilience a habitual operational mindset, while multi-layered connectivity systems would serve both as a deterrent against coercive disruptions and as a confidence-building mechanism, reinforcing societal trust in the state's ability to maintain essential functions under pressure.

2. Institutionalizing Digital Continuity of Governance

Ukraine demonstrates that a unified digital platform—integrating identity

verification, administrative services, taxation, and access to official documents—ensures citizens remain connected to the state even during crises. Such platforms are not merely administrative tools; they serve as strategic infrastructure for governance, societal cohesion, and national resilience. Taiwan can proactively develop a similarly integrated digital system to maintain core government functions—civil registration, social services, and emergency communications—without relying solely on physical offices, which may be disrupted during conflicts or disasters. For example, during the COVID-19 pandemic, Taiwan implemented the Instant Mask Map, providing real-time information on the availability of face masks nationwide. The Central Epidemic Command Center also published daily updates to ensure citizens had access to reliable information, while traditional media channels—TV, radio, and broadcasts—continued to maintain communication with the public. Furthermore, multi-channel integration—including mobile, web, and AI-assisted services—combined with a robust public–private partnership ecosystem, can efficiently scale service delivery while providing redundancy in case of partial system outages.

3. Defending the Cognitive Domain: Taiwan in a Gray-Zone Battlefield

China's approach to Taiwan remains firmly within the gray-zone spectrum, emphasizing persistent cognitive warfare rather than overt kinetic confrontation. Leveraging local proxies, linguistic familiarity, and social narratives aimed at creating fragmentation, Beijing seeks to erode public trust and shape perceptions in subtle but pervasive ways. Ukrainian experience demonstrates that building resilience across the cognitive domain requires a comprehensive, whole-of-society system. This system integrates government institutions, media organizations, civil society, and broadcast networks into a coordinated, multi-layered defense capable of early warning, rapid verification, and sustained public engagement.

For Taiwan, establishing a credible "digital shield" begins with cultivating public trust. This includes fostering transparent, timely communication through trusted media and public figures, complemented by robust civil society participation. Civilian-led initiatives—ranging from independent fact-checking NGOs to crowdsourced reporting platforms—can act as rapid-response forces to detect and counter disinformation before it spreads widely. Strengthening public-private coordination is essential: AI-assisted real-time disinformation monitoring, Deepfake detection labs, and collaboration with social media platforms can ensure that verified information is amplified while coordinated influence operations are disrupted.

Equally critical is empowering autonomous social groups to act as decentralized

nodes of detection and response, leveraging collective societal capacity to identify, verify, and respond to emerging threats. Over the long term, civic digital literacy must be treated as part of the nation's security infrastructure, embedding media literacy, critical thinking, and verification skills into education and public awareness campaigns. By integrating these layers—strategic government oversight, civil society engagement, technical verification, and citizen empowerment—Taiwan can construct a resilient cognitive defense posture capable of withstanding sustained gray-zone influence operations.

IV. CONCLUSION

Ukraine's experience demonstrates that digital resilience is far more than a technical challenge; rather, it constitutes an integrated capability grounded in domestic capacity, wartime adaptation, and external support, enabling the sustained functioning of institutional systems while preserving societal, military, and informational advantages under the extreme pressures of wartime. Beyond maintaining connectivity or defending networks, resilience encompasses the ability to preserve governance continuity, coordinate rapid civil and military responses, and safeguard the integrity of truth in the information environment. For Taiwan, these lessons underscore the importance of building a proactive, whole-of-society digital resilience strategy. By combining democratic governance, technological agility, and societal trust, Taiwan can cultivate a "digital fortress island" capable of withstanding gray-zone operations, protecting its information environment, and maintaining strategic advantage even under sustained hybrid threats. In essence, Ukraine's experience offers a blueprint: digital resilience is not only about networks or devices—it is a national capability rooted in foresight, coordination, and the empowerment of both institutions and citizens.

Blinding Manila: The Invisible Siege of the South China Sea

*Dr. Siông-Ui Frederick Tsiam**

On June 17, 2024, a violent confrontation at Second Thomas Shoal left a Philippine Navy sailor severely injured. Yet, while global attention fixed on the visceral images of machetes and water cannons, a quieter, more insidious contest was unfolding in the ether. Philippine crews reported screens going dark, radios filling with static, and GPS coordinates drifting aimlessly. This episode illustrates an emerging pattern in China's approach: physical clashes at the surface increasingly coincide with systematic attempts to blind and distort the battlespace in the electromagnetic spectrum.

Since 2012, Beijing has aggressively challenged the Philippines' Exclusive Economic Zone （EEZ）. More recent dynamics, however, reveal a critical evolution in strategy: China has graduated from relying primarily on "kinetic deterrence" to integrating what this article terms "spectrum siege." By layering electromagnetic spectrum （EMS） suppression over physical coercion, Beijing seeks to degrade Manila's ability to monitor and publicise maritime incidents and thereby incrementally expand its de facto control over key contested waters in the South China Sea.

Manila's "naming and shaming" strategy relies on a digital lifeline: the ability to promptly document and broadcast footage of Chinese coercive behaviour to the world. Beijing's counteroffensive is designed to strain this link. By electronically isolating Philippine vessels, China aims to erode operational transparency at the point of contact, limiting Manila's capacity to produce timely, verifiable evidence of frontline realities.

* Dr. Tsiam is an Assistant Research Fellow at the Institute for National Defence and Security Research (INDSR). He holds a PhD from the Graduate Institute of International Affairs and Strategic Studies at Tamkang University. Dr Tsiam's primary research areas include geostrategy, maritime security, and wargaming, with a specific focus on electronic and hybrid warfare.

I. KEY CONCEPTS: SPECTRUM SIEGE AND TRANSPARENCY DENIAL

In recent years, Western defence communities and think tanks have paid growing attention to how China and Russia employ electromagnetic spectrum operations （EMSO） and spectrum manipulation as tools of nonkinetic coercion in the grey zone.[1] Building on joint doctrine that frames EMSO as military actions to exploit, attack, protect, and manage the electromagnetic environment,[2] a wide range of analyses now examine how adversaries use jamming, spoofing, and GNSS denial to shape operational behaviour short of war. However, much of this literature focuses on cataloguing technical capabilities and documenting threat trends, rather than on how these activities interact with maritime transparency mechanisms and alliance commitments in specific theatres such as the South China Sea.

Against this backdrop, the present article introduces two operational concepts—"spectrum siege" and "transparency denial"—to analyse China's evolving grey zone strategy in the South China Sea. Rather than claiming to discover an entirely new form of warfare, the article builds on existing EMSO and grey zone scholarship and adapts it to the specific problem of how Beijing degrades Manila's ability to observe, document, and publicise coercive behaviour at sea. Whereas traditional A2/AD analysis emphasises missile salvos and kinetic exclusion, spectrum siege highlights the cumulative effect of routine jamming, spoofing, and interference in making navigational and informational conditions so uncertain that access becomes prohibitively risky even in "peacetime." Transparency denial, in turn, captures the deliberate use of these EMSO tools to obstruct, manipulate, or delay the information flows that underpin the Philippines' "naming and shaming" strategy and allied decisionmaking.[3]

The article also adapts the notion of a "kill web" to describe a distributed network of PLA, China Coast Guard, and maritime militia platforms that share ISR,

1. Selena Lin, "Electronic Warfare and Crisis Stability in the US-China GrayZone Competition," *Marcellus Policy Analysis*, Fall 2025, https://jqas.org/wp-content/uploads/2026/02/Lin-Analysis.pdf; "China's Spratly ISR and EW Upgrades," *Asia Maritime Transparency Initiative,* December 2, 2025, https://amti.csis.org/chinas-spratly-isr-and-ew-upgrades/.
2. U.S. Joint Chiefs of Staff, *Joint Electromagnetic Spectrum Operations, Joint Publication 3-85* (Washington, DC: Joint Chiefs of Staff, May 22, 2020), https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_85.pdf.
3. Mark Harris, "Ghost Ships, Crop Circles, and Soft Gold: A GPS Mystery in Shanghai," *MIT Technology Review,* November 15, 2019, https://www.technologyreview.com/2019/11/15/131940/ghost-ships-crop-circles-and-soft-gold-a-gps-mystery-in-shanghai/; J. Michael Dahm, *Electronic Warfare and Signals Intelligence* (Laurel, MD: Johns Hopkins University Applied Physics Laboratory, 2020), https://apps.dtic.mil/sti/trecms/pdf/AD1128255.pdf.

EW, and targeting functions via overlapping sensors and communications links. Over time, persistent EMS activity by this network creates what the article calls an "electromagnetic maritime baseline": a background level of surveillance and interference that normalises exclusionary control below the threshold of armed conflict. This framing builds on PLA concepts of "informationised" and "intelligentised" warfare by highlighting how cyber-electromagnetic operations are embedded in day-to-day law enforcement and grey zone practices at sea.

II. THE INVISIBLE SIEGE: BLINDING MANILA'S EYES AND EARS

China's electronic warfare capabilities are not merely theoretical; they are increasingly visible in operational settings. During the regionally held "Talisman Sabre" exercises, China's Type 815G electronic surveillance ships were observed operating in the vicinity, with analysts assessing that they were likely collecting electromagnetic signatures of allied vessels.[4] Since the Philippine Navy and Coast Guard operate platforms largely sourced from the United States and Japan, many of their key signatures are plausibly already catalogued. Compared with its allies, the Philippines has relatively limited electronic protection （EP） capabilities, making its frontline units particularly vulnerable to China's emerging EMS operations.

First is navigation denial. The Asia Maritime Transparency Initiative （AMTI） has documented that China has deployed fixed and mobile radar and electronic warfare systems on its artificial islands, including Mischief Reef and Fiery Cross Reef.[5] Opensource modelling and interference protection criteria suggest that, from a location such as Mischief Reef, a tacticallevel jamming source on the order of tens to lowhundreds of watts could be sufficient to disrupt civiliangrade GPS/GNSS receivers on Philippine vessels operating roughly 30 kilometres away at Second Thomas Shoal. Mounted on elevated infrastructure and combined with directional antennas, such systems can create localised "cones of silence" in which L1 and L2 signals fall below usable thresholds for nonhardened navigation equipment.[6]

A mobile tactical jammer mounted on a CSK181 chassis, or comparable platforms, could be used to execute this form of localised denial, even before

4. James Goldrick, "China's Intelligence Gathering Ships Change the Equation," *Lowy Institute,* July 31, 2019, https://www.lowyinstitute.org/the-interpreter/china-s-intelligence-gathering-ships-change-equation.

5. Asia Maritime Transparency Initiative, "China's Spratly ISR and EW Upgrades," *CSIS,* December 2, 2025, https://amti.csis.org/chinas-spratly-isr-and-ew-upgrades/.

6. J. Michael Dahm, *Electronic Warfare and Signals Intelligence*.

considering the higherpower systems that can be supported by the islands' militarised power grids. The construction of high towers and other elevated structures on these features appears designed, among other purposes, to mitigate lineofsight limitations and extend the effective range of such systems. Philippine Coast Guard statements and media reporting indicate that local vessels have experienced not only suspected jamming but also apparent AIS spoofing in these waters.[7]

Second is tactical isolation and digital fabrication. Beyond jamming, Beijing increasingly targets tactical communications in the AIS （161.975/162.025 MHz） and voice （around 156 MHz） bands. Jamming VHF voice channels—such as Channel 16 used for distress calls—is technically straightforward and has been reported in multiple encounters near Second Thomas Shoal.[8] Because AIS packets are broadcast in the clear on standardised VHF channels, even relatively lowpower transmitters can inject large volumes of fabricated messages into the local traffic picture, a vulnerability already documented in technical studies of AIS spoofing and system resilience.[9]

This combination of jamming and spoofing can generate several tactical effects. First, it disrupts maritime awareness. By generating "ghost ships," an actor can create a false picture of overwhelming numbers to psychologically pressure Philippine commanders, or conversely, clutter the display to mask the presence of its own vessels and delay tactical responses.[10]

Second, it enables digital lawfare. AIS manipulation makes it technically possible to fabricate digital traces showing Philippine vessels "intruding" into restricted waters or performing dangerous manoeuvres, providing a putative legal pretext for "law enforcement" actions. Finally, it creates navigational lures. When combined with GPS spoofing, manipulated AIS data can mislead Philippine crews into believing they are in safe waters when they are in fact drifting toward shoals or into tactically disadvantageous positions, especially under conditions of poor visibility or operational stress.

---

7. "Philippine Coast Guard Accuses China of Using AIS Spoofing to Mislead Authorities," *Marine Insight,* December 16, 2024, https://www.marineinsight.com/shipping-news/philippine-coast-guard-accuses-china-of-using-ais-spoofing-to-mislead-authorities/.
8. "Chinese Ship Jams Communications as Filipino Forces Deliver Supplies to Philippines-Occupied Shoal," *Arab News*, November 18, 2025, https://arab.news/423uy.
9. Cyril Ray, Clément Iphar, Aldo Napoli, Romain Gallen, Alain Bouju. *DeAISproject: Detection of AIS Spoofing and Resulting Risks,* MTS/IEEE OCEANS'15, IEEE, May 2015, Gênes, Italy, https://minesparis-psl.hal.science/hal-01166151v1/document.
10. Charie Abarca, "PCG: China Using AIS Spoofing to Mislead Public and Stir Confusion," *Inquirer.net,* December 13, 2024, https://globalnation.inquirer.net/258190/pcg-china-using-ais-spoofing-to-mislead-public-and-stir-confusion.

Third is strategic silencing. Perhaps most critically, China appears to be targeting the commercial satellite uplinks （Inmarsat, VSAT, etc） that Philippine crews rely on to upload imagery and video evidence. Unlike hardened military systems with frequencyhopping capabilities, commercial terminals are vulnerable to relatively simple forms of broadspectrum noise. By raising the bit error rate just enough to intermittently sever these connections, an adversary can ensure that, while the physical clash occurs in real time, the flow of verifiable information is delayed — or, in some cases, lost entirely.

Targeting commercial Lband or Ku/Kaband links is technically less demanding than degrading hardened military systems. Commercial terminals typically lack the electronic countercountermeasures（ECCM）— such as frequency hopping — found in military gear. A coast guard cutter or auxiliary vessel emitting broadspectrum noise can raise the bit error rate sufficiently to disrupt throughput on nearby civilian SATCOM terminals.[11] Given that China has already demonstrated the ability to interfere with militarygrade GPS signals on US RQ4 drones,[12] disrupting commercial SATCOM terminals on lightly protected civilian or coast guard vessels is well within its demonstrated technical reach and is likely to be significantly easier from an operational standpoint.

III. ANATOMY OF A KILL WEB

China's emerging positional advantage in the South China Sea rests on a theatre-wide "kill web" that integrates military and non-military assets into a progressively denser network of sensors and emitters.

Island fortresses. AMTI reporting indicates that China has successively installed clusters of fixed monopole antennas at multiple locations, notably Subi, Mischief, and Fiery Cross Reefs. In addition to large concrete pads, commercial imagery suggests the presence of vehiclemounted sensor systems potentially configured for specific spectrum bands. Whether employed primarily for ISR or for selected suppression roles, this infrastructure provides essential "backend computational" support and contributes to widearea coverage for surveillance and electromagnetic effects.

---

11. Alakananda Paul, et. al., "Interference Protection Criteria," NTIA Report 05-432, *US Department of Commerce*, https://www.ntia.gov/files/ntia/publications/ipc_phase_1_report.pdf.
12. Bill Gertz, "Chinese Military Using Jamming Against U.S. Drones," *The Washington Free Beacon*, May 22, 2015, https://freebeacon.com/national-security/chinese-military-using-jamming-against-u-s-drones/.

Militarised coast guard. The China Coast Guard is no longer just a lawenforcement agency. A notable example is the transfer of Type 056 corvettes from the PLA Navy（PLAN）to the CCG. While missile launchers were removed, these vessels retained their SR64 air/surface search radars and associated firecontrol systems, as well as bridgemounted antennas assessed to support electronic warfare and signals intelligence functions. Such platforms can, in principle, detect and interfere with commercial drone frequencies and some military radars. The 12,000ton Zhaotou-class cutters also serve as major SIGINT and commandandcontrol nodes within this network.

Figure: CCG 3104.

Source: "Sabina Shoal: A Dangerous New Flashpoint is Fast Emerging in the South China Sea," *CNN*, https://edition.cnn.com/2024/08/27/asia/china-philippines-new-flashpoint-sabina-shoal-intl-hnk.flashpoint-sabina-shoal-intl-hnk.

Maritime militia. Tasked with challenging peripheral waters and asserting presence, these ostensibly civilian fleets can contribute to "distributed jamming" and "spectrum saturation." Drawing on opensource analyses, Chinese maritime militia units have been reported to employ highpower VHF and HF transceivers and modified radar reflectors, enabling them to clutter radar images, mask specific frequency bands, and complicate target discrimination. By altering hull structures or adding reflectors to increase radar crosssection（RCS）, smaller fishing vessels can appear as larger ships on an opponent's sensors, potentially misleading tactical judgment and slowing decisionmaking.[13]

13. Andrew S. Erickson, Conor M. Kennedy, "China's Maritime Militia," *andrewerickson.com,* March 7, 2016, https://www.andrewerickson.com/wp-content/uploads/2016/06/Maritime-Militia_Chinas_Erickson-Kennedy_CNA_20160307.pdf.

Air and space layer. The final layer is multidimensional support from air and space. Leveraging extended runways on major reefs, PLAN and PLAAF specialmission aircraft（including Y8/Y9 electronic warfare variants）reportedly maintain more regular rotations over the southern theatre. These platforms carry highpower airborne EW systems that can conduct standoff jamming and serve as “aerial data relays,” passing frontline data back to rear command centres and thereby shortening the kill chain. Above them, the BeiDou Navigation Satellite System （BDS） provides a unique shortmessage communication function, offering Chinese vessels a resilient, encrypted backup link even in heavily contested electromagnetic environments.

IV. SILENT EXPANSION: DE FACTO SEA CONTROL

Since assuming power, Xi Jinping has identified “building a maritime power”[14] as a critical element in realising the “Chinese Dream”[15] and the “Great Rejuvenation of the Chinese Nation”. Beyond large-scale aircraft carrier construction, Beijing has actively pursued anti-access/area-denial（A2/AD）capabilities. While in the northern seas this architecture is heavily missilecentric, in the South China Sea it increasingly relies on nonlethal but potent electronic warfare and related tools as key means of shaping access and imposing costs.

Modern sea control is less about fleetonfleet battles and more about establishing exclusionary zones that influence behaviour. China’s emerging “spectrum blockade” concept seeks to make navigation and communication in certain areas sufficiently risky and uncertain that commercial and government actors selflimit their presence. Much like the Red Sea crisis forced shipping to reroute due to prohibitive insurance costs, China’s nonlethal EW activities can, under certain conditions, create a “highrisk area” that in practice constrains the Philippines’ operational freedom without a formally declared blockade.[16]

---

14. 〈習近平的海洋情懷〉，《中新網》，2018 年 6 月 5 日，https://www.chinanews.com.cn/m/gn/2018/06-05/8530695.shtml。

15. 〈習近平在中共中央政治局第八次集體學習時強調 進一步關心海洋認識海洋經略海洋 推動海洋強國建設不斷取得新成就〉，《共產黨員網》，2013 年 7 月 31 日，https://cpc.people.com.cn/BIG5/n/2013/0731/c64094-22399483.html。

16. Same effect applies to Taiwan. 詹祥威，〈紅海危機與全球航運安全觀察〉，《國防安全即時評析》，2025 年 7 月 17 日，https://indsr.org.tw/focus?uid=11&pid=2870&typeid=27。

Since 2023, a series of incidents — including the use of militarygrade lasers, such as CCG 5205 temporarily blinding[17] Philippine crew members,[18] and reported AIS spoofing events that generated confusion over vessel locations,[19] — have highlighted a pattern of coercive actions in the electromagnetic and optical domains. In the same period, Philippine reporting has pointed to increased cyber and electronic attacks against public vessels, disrupting rotation and resupply（RORE）missions,[20] while navy officials have stated that their ships have faced "electronic interference" in these waters for the past three to four years.[21]

Beijing now explicitly frames the "cyber and electromagnetic domains" as extensions of national sovereignty, crucial for maintaining national security and global influence. This conceptualisation has translated into the use of cyber infiltration and electronic jamming as tools of sovereign defence, deterrence, and ideological competition.[22] Combined with persistent activities around disputed features, these practices are contributing to a zone of exclusionary maritime control that falls below the traditional thresholds of open war yet steadily alters the operational status quo.

V. GRAY ZONE, RED LINES: THE ALLIANCE DILEMMA

China's emerging spectrumcentric strategy presents a significant challenge to the *US–Philippines Mutual Defense Treaty*（MDT）. International practice and expert restatements such as the Tallinn Manual 2.0 generally apply an "effectsbased"

17. Brad Lendon, "Philippine Coast Guard Says Chinese Ship Aimed Laser at One of Its Vessels," *CNN,* February 13, 2023, https://edition.cnn.com/2023/02/13/asia/philippines-china-coast-guard-laser-intl-hnk-ml.
18. Raymond Carl Dela Cruz, "China Coast Guard Points Laser Light at PCG Ship Off Ayungin," *Philippine News Agency,* February 13, 2023, pna.gov.ph/articles/1195090.
19. GMA Integrated News, "PCG Alleges 'Spoofing' After China Coast Guard Vessel Tracked in Zambales, But Actually in HK," *GMA News,* December 13, 2024, https://www.gmanetwork.com/news/topstories/nation/929942/pcg-alleges-spoofing-after-china-coast-guard-vessel-tracked-in-zambales-but-actually-in-hk/story/.
20. Michael Punongbayan, "Navy Confirms Increased Cyberattacks in West Philippine Sea," *The Philippine Star,* February 28, 2024, https://www.philstar.com/headlines/2024/02/28/2336705/navy-confirms-increased-cyberattacks-west-philippine-sea.
21. Bianca Dava, "Interference on PH Navy Ships' 'Electronic Capabilities' in West PH Sea Ops 'Has Been Going on for 3 to 4 Years'," *ABS-CBN News*, February 27, 2024, https://www.abs-cbn.com/news/2024/2/27/ph-navy-monitoring-interference-on-ships-electronic-capabilities-in-west-ph-sea-1725.
22. Ho Ting Hung, "Exploring China's Cyber Sovereignty Concept and Artificial Intelligence Governance Model: a Machine Learning Approach," *Journal of Computational Social Science,* Vol.8, No.24, January 4, 2025, https://link.springer.com/article/10.1007/s42001-024-00346-8.

test to determine whether a cyber or electronic operation constitutes a "use of force." Actions that result in death, injury, or physical damage may qualify as an "armed attack."[23] China's operations in the South China Sea appear calibrated to stay just below this threshold: its EW activities are designed to produce "functional paralysis"—temporary loss of navigation and communications—rather than direct physical destruction, while physical harm is typically inflicted through "cold weapons" such as water cannons and ramming. This pattern creates a legal grey zone in which the conditions for invoking Article IV of the MDT remain contested, granting Beijing considerable room for manoeuvre and strategic initiative.

Even though Washington has repeatedly stated that armed attacks on Philippine public vessels would trigger treaty obligations, definitional ambiguity over what constitutes an "armed attack" in the cyberelectromagnetic domain complicates timely and credible responses. An overly expansive interpretation risks drawing the United States into a legal and political quagmire over rules of engagement（ROE）, while an overly narrow one risks eroding alliance credibility. China's longterm pattern of "lowintensity, highfrequency" operations thus serves two purposes: it reduces the likelihood of a clearcut treaty trigger while gradually establishing an "electromagnetic maritime baseline" of exclusionary control that normalises higher levels of risk for Philippine forces.

VI. A REHEARSAL FOR THE TAIWAN STRAIT

The South China Sea increasingly functions as a testing ground. The tactics employed against the Philippines today—AIS spoofing, GPS denial, and SATCOM jamming—could, in a future contingency, be adapted and scaled for use against Taiwan. By expanding these pointdefence tactics into a widerarea "electromagnetic quarantine," Beijing could seek to disrupt the navigation and communications of energy tankers and cargo ships bound for Taiwan and nearby transshipment hubs.

In a worstcase scenario, sustained interference of this kind could create an "electromagnetic black hole" in critical shipping lanes, forcing ships to abandon routine reliance on digital navigation and revert to more rudimentary methods. More importantly, persistent uncertainty about navigational safety and communications reliability could prompt marine insurers and shipping lines to reassess coverage

23. Michael N. Schmitt, "Rewired Warfare: Rethinking the Law of Cyber Attack," *International Review of the Red Cross*, Vol. 96, No. 893, 2014, p. 189206, https://international-review.icrc.org/sites/default/files/irrc-893-schmitt.pdf.

and routing, gradually constraining Taiwan's economic lifelines through market mechanisms. Without declaring a formal blockade or firing a missile, China could, in theory, use spectrum suppression combined with commercial risk calculations to marginalise a globally interconnected island economy. This section is forwardlooking and extrapolates from current patterns rather than describing an already operational campaign.

VII. FIGHTING BACK IN THE ETHER

Recent naval developments — from Japan's *Mogami*-class to Australia's *Hunter*-class frigates — signal a wider shift: in highend maritime competition, spectrum control increasingly rivals, and in some missions outweighs, sheer displacement. The likely victor in future naval warfare will be the side that best optimises SWaPC（Size, Weight, Power, and Cost）to generate resilient sensing, communications, and electronic warfare power across contested bands.

Taiwan, as a critical node in the First Island Chain, is well placed to champion a regional "Electromagnetic Spectrum Cooperation Mechanism" built around three pillars.

Common Spectrum Operating Picture（CSOP）. Taiwan, the United States, South Korea, Japan, the Philippines, New Zealand, and Australia should move toward integrating selected spectrummonitoring data. When a Taiwanese frigate detects a distinctive jamming waveform from a Chinese militia vessel in northern waters, that information should be shared nearrealtime via encrypted datalinks with a Philippine patrol ship or a Japanese destroyer. Such triangulation and crossverification would allow allies to distinguish deliberate jamming from technical malfunction and to expose spoofing attempts quickly, sharply reducing the effectiveness of China's informationasymmetry tactics.

Shared Electronic Order of Battle（EOB）. Allies should jointly build a library of acoustic and electronic signatures — "fingerprints" — with particular emphasis on Chinese paramilitary vessels operating under civilian cover. Once a vessel's electronic fingerprint is positively identified by one ally, it can be flagged as a threat or highrisk contact across the entire network, raising the political and operational costs of China's camouflage and grey zone operations.

Resilient PNT. Given the growing normalisation of GPS denial and spoofing in the South China Sea, regional states need to standardise and diversify alternative positioning, navigation, and timing（PNT）solutions. Beyond strengthening inertial navigation systems（INS）, they should accelerate testing and fielding of

lowEarthorbit PNT（LEOPNT）and signalofopportunity（SoOP）approaches, so that commercial and government vessels can maintain safe operations even under sustained Chinese electromagnetic pressure.

The window to secure the electromagnetic spectrum is closing. If Washington and its allies cannot credibly ensure that a Philippine sailor can trust his navigation solution or call for help under electronic duress, they risk losing the contest for the South China Sea without a single missile being fired.

SUBMISSION

Defense Security Brief (DSB) is a semiannual publication, open access, and peer-reviewed journal published by the Institute for National Defense and Security Research (INDSR) Taipei, Taiwan. Established in 2011, DSB was originally founded by the Ministry of National Defense and continued by the INDSR from 2018. We aim at strengthening research collaboration and fostering exchanges between researchers and experts both domestically and internationally.

DSB publishes original papers, reviews, comments and case studies. Contributions that engage with contemporary international affairs, defense, security, strategy, Indo-Pacific issues and policy reviews are particularly welcome.

All manuscripts must be in English and should be submitted via email to publication@indsr.org.tw. Please note that the editorial review process can take up to three months. For further information and previous volumes, please visit the official website of DSB:
https://indsr.org.tw/en/download/2/DEFENSE-SECURITY-BRIEF

GENERAL GUIDELINES

Authors are advised to follow these guidelines:

- All manuscripts should be between 1,500 - 2,500 including footnotes.
- Citation tyle: *The Chicago Manual of Style*, 16th edition.
- Co-authorship is allowed.
- A short author's biography no more than 100 words need to be provided but not be included in the manuscript.
- An honorarium is provided upon successful publication up to NT$ 7,500 (NT$3,000/1,000 words per paper).
- For any further information, please email the Associate Editor, Dr. William Chih-tung Chung, at *publication@indsr.org.tw.*

Institute for National Defense and Security Research