

The War of Spies: How China's Intelligence Services Are Infiltrating Taiwan—and What Europe Must Learn from It

間諜之戰：中國情報機構如何滲透臺灣 ——兼論對歐洲的啟示

Jürgen Kremb (周勁恆)*

Journalist and Author; Taiwan Fellow 2025; Visiting Scholar, Human Rights Institute,
Soochow University (東吳大學人權研究所), Taipei

Abstract

This study examines the People's Republic of China's (PRC) systematic preparations for a potential conflict with Taiwan and, beyond that, with Western democracies. Drawing on academic literature, primary sources, Taiwanese security agency reports, international think tank studies, and background discussions with intelligence and government experts in the Republic of China (ROC), the analysis addresses how Chinese security and intelligence services influence, infiltrate, and destabilize Taiwan's strategic, psychological, and social landscape. The central thesis

* Jürgen Kremb is a visiting scholar in the Human Rights Program at Soochow University in Taipei, where he conducts research on Chinese intelligence services and hybrid warfare. He was a recipient of the Taiwan Fellowship 2025 and holds an MA in East Asian Studies and Journalism from Freie Universität Berlin. For more than 20 years, he headed the foreign bureaus of the German news magazine DER SPIEGEL in Beijing, Vienna, and twice in Singapore. He wrote several thousand articles for numerous media outlets in German-speaking countries. Kremb has also published books on security services, such as the German Federal Criminal Police Office (BKA), and the first biography of the Chinese dissident Wei Jingsheng. He is considered an expert on Chinese security issues and Islamism in Southeast Asia. He was expelled from China in 1998 for his critical reporting.

is that Taiwan serves as the “laboratory” for Chinese influence operations in the 21st century: the methods Beijing tests in Taiwan serve as a model for global application against democratic states, particularly in Europe and the United States. Classic intelligence operations, United Front work, cognitive warfare, and hybrid influence strategies combine to form a comprehensive “overall operation” that goes far beyond traditional espionage. Taiwan is thus not only a stage but a testing ground for a new form of political-strategic confrontation whose primary goal is not only military conquest but the psychological paralysis of the adversary.

Key words: cognitive warfare; Taiwan; Chinese intelligence services; hybrid warfare; spy warfare.

I. Introduction: China's Strategy Toward Taiwan

Taiwan is far more than a territorial target for the People's Republic of China (PRC). The island serves as a global testing ground for a new form of conflict—"cognitive warfare"—that aims to manipulate the consciousness, perceptions, and decision-making behavior of Taiwanese society as a whole. Unlike traditional espionage, this comprehensive strategy combines classical intelligence methods with modern psychological operations to destabilize Taiwan from within without firing a single shot. The openness of Taiwanese democracy is exploited as a gateway to sow distrust in state institutions and undermine social cohesion. This study examines the operational architecture of that strategy: who conducts it, through what methods, and what Taiwan and Europe can learn from it.

The author brings particular professional experience to this subject. Having served as bureau chief of the German news magazine *Der Spiegel* in Beijing (1990–1998), Vienna (2003–2005) and twice in Singapore (1998–2002, 2005–2013) and subsequently as a correspondent reporting on Asian security services, he observed Chinese surveillance and intelligence operations firsthand—up to and including his own expulsion from the PRC in November 1998 following an office raid by eight intelligence agents.¹ This study was conducted as part of the Taiwan Fellowship 2025, with research carried out in Taipei in close cooperation with Taiwanese security and intelligence experts, including representatives of the Ministry of Justice Investigation Bureau (MJIB, 法務部調查局), the National Security Bureau (NSB, 國家安全局), the Military Intelligence Bureau (MIB, 國防部軍事情報局), and affiliated think tanks.

That the threat posed by Chinese agents in Taiwan is already part of everyday life was illustrated strikingly early in the research period. In May 2025, a woman with a strong PRC accent approached the author's group at Alishan, a well-known tourist destination in central Taiwan. Despite Beijing's ban on issuing exit permits for PRC citizens to travel to Taiwan, the woman claimed to reside in northern Denmark—in a region close to the strategically important Skagerrak waterway, through which all

¹ Jürgen Kremb, "Maul halten, hier ist China," *Der Spiegel*, No. 48 (1998/11/22). (Engl: "Shut up, here is China.")

shipping traffic from the Baltic Sea to the North Sea passes. The author terminated the conversation. Shortly after, the woman was seen speaking into her phone in a northern Chinese dialect, and then followed the group to their hotel. Upon return to Taipei, the author contacted the relevant unit of the MJIB. Surveillance footage from street cameras confirmed that the woman had followed the group into their hotel lobby; immigration records showed she had departed Taiwan the following day. The MJIB subsequently notified both the German BND resident at the German mission in Taipei and Denmark's intelligence service. The case was also discussed at the National Security Council (國家安全會議).

Taiwan's intelligence services are highly valued in the West precisely because of their specific and irreplaceable expertise on China. It is no coincidence that Germany's Federal Intelligence Service (BND) has maintained close cooperation with the NSB in Taipei since the early 1960s.² Despite the Federal Republic's establishment of diplomatic relations with the PRC in 1972, this cooperation was never significantly impaired—on the contrary, the BND office in Taipei saw its staff increased in recent years. Yet as Taiwanese society became more democratic, its security services appeared for a period to have underestimated the existential nature of the infiltration challenge. It was not until January 2024 that the MJIB established its Cognitive Warfare Research Center (法務部調查局認知戰研究中心), merging several departments into a powerful combined unit specifically tasked with these responsibilities.³

II. Conceptual Framework:

Cognitive Warfare, United Front, and Hybrid Threats

1. Cognitive Warfare: Beyond FIMI

In Taiwan's security debate, two experts have emerged who combine academic excellence with direct operational experience: Professor Kerry Gershaneck, a longtime

² Chen Chern (陳志宏), "The Intelligence Connection between West Germany and Taiwan: An Unknown Chapter of the Cold War" (2025/12/6), visited date: 2026/3/10, *Academia Sinica Newsletter*, <https://newsletter.sinica.edu.tw/reviews/file/file/121/12117.pdf>.

³ "Research Center Set Up to Combat Cognitive Warfare" (2024/1/19), visited date: 2026/3/8, *Taipei Times*, <https://www.taipeitimes.com/News/front/archives/2024/01/19/2003812310>.

Pentagon strategist whose expertise in strategic communication has been explicitly recognized by President Lai Ching-te,⁴ and Professor Liu Wen-ping (劉文斌), the former head of the research department at the MJIB and the most widely cited expert on the anatomy of Chinese influence operations.

Professor Liu is particularly critical of the “Foreign Information Manipulation and Interference” (FIMI) approach, which is popular in Europe and used by the European External Action Service (EEAS). According to Liu’s analysis, FIMI simultaneously falls short and is too vague: a Taiwanese advertising campaign for oolong tea—manipulating information to influence consumer behavior and shift market shares—would, by strict FIMI logic, constitute cognitive warfare against Europe.

Building on classical persuasion models from communication research, Liu proposes the “AAAB model” (Abroad, Adversaries, Attack, Benefits) to conceptualize the mechanisms through which information operations influence cognitive processes and ultimately shape behavior: “Foreign adversaries disseminate information for political purposes to target specific groups and individuals, alter their cognition, and consequently influence their words and deeds in a way that benefits the adversary.”⁵ This approach clearly distinguishes cognitive warfare from legitimate soft power by focusing on the malicious political objective and the targeted behavioral change, not merely on the act of information dissemination.

2. The United Front: Instrumental Friendship

A persistent misunderstanding is the reduction of United Front work to the Maoist mantra of “winning over secondary enemies to defeat the main enemy.” Liu clarifies that the CCP also “co-opts allies to defeat the main enemy.” The United Front (統一戰線), one of Mao Zedong’s three “magic weapons” (法寶)—alongside the Red Army and party building—is not a traditional intelligence service but a political mobilization apparatus. Liu defines it with precision: “The Communist Party forms friendships with

⁴ Kerry Gershaneck, *Political Warfare: Strategies for Combating China’s Plan to ‘Win Without Fighting’* (Quantico: Marine Corps University Press, 2020).

⁵ Liu Wen-ping (劉文斌), “Research on Negative Effects and Responses to Cognitive Warfare,” *Nanhua Social Science Forum* (Chiayi), Vol. 16 (July, 2024), p. 70.

people outside the party in order to mobilize these friends to support the party's political goals.”⁶

The concept of “instrumental friendship” is key to understanding how the United Front differs from classical espionage. While espionage (間諜, Spy War) operates in the shadows to steal secrets, the United Front operates in broad daylight within civil society, aiming to corrupt decision-making processes and create an internal layer of collaborators—what research sometimes calls “unwitting collaborators.” In practice, the two systems form a symbiosis: the United Front often serves as the legal cover network in which potential agents are identified, vetted, and subsequently recruited for more overtly covert operations. Espionage thus uses the structures of the United Front as an operational precursor.

3. Hybrid Warfare and the Gray Zone

Hybrid warfare combines conventional military threats with non-traditional means such as psychological warfare, economic coercion, and cyberattacks in a manner that defies easy temporal classification: it operates in a permanent gray zone in which there is no clear separation between peace and war. The RAND Corporation identifies “salami-slicing” as a central element of this gray zone—small, hard-to-track provocations that individually do not justify military retaliation but, taken together, shift the status quo in Beijing's favor.⁷ Current examples include the cutting of undersea cables in the waters around Taiwan and the disabling of Automatic Identification Systems (AIS) on civilian ships near Kinmen.⁸

Professor Liu's analytical contribution lies in mapping the interaction of these spheres across four conflict phases: in the peace phase, soft power campaigns and the cultivation of “instrumental friends” lay the groundwork for networks that can be activated in an emergency. In the gray zone phase, cognitive warfare intensifies through

⁶ “The Origin of the Concept of the United Front,” visited date: 2018/8/22, 《*Luoyang Normal University United Front Work Department*》, <https://sites.lynu.edu.cn/tzb/info/1008/1223.htm>.

⁷ RAND Corporation, *Chinese Influence Operations in the Indo-Pacific* (Santa Monica: RAND, 2024).

⁸ Yang Tai-yuan, “The Meaning and Development Trend of the PLA's ‘Gray Zone Harassment’ in the Waters Around Taiwan” (2024/5/28), visited date: 2025/11/15, 《*China Studies Institute*》, <https://iccs.org.tw/NewsContent/188>.

the dissemination of narratives such as “anti-Americanism” (疑美論) or systematic defamation of the Taiwanese armed forces’ combat effectiveness, designed to undermine public confidence in the country’s own defense capabilities. In the war phase, the cognitive component aims to demoralize the civilian population and political leadership to provoke poor decision-making. In the post-war phase, cognitive warfare transforms into a “cognitive civil war” within occupied territory to legitimize a new order and suppress resistance from inception.

III. The Architecture of Infiltration: History and Institutional Structure

1. Historical Roots: Zhou Enlai and the Teke

The history of Chinese intelligence services is inseparable from the paranoia and ruthlessness of an underground organization that has, since its inception, operated according to a revolutionary logic in which morality is subordinate to absolute party discipline. After the CCP’s split with the Kuomintang (KMT) in 1927, Zhou Enlai created the Teke (特科)—the CCP’s first systematic intelligence apparatus. Its most notorious unit, the “Red Brigade” (紅隊), operated as an execution squad. The 1931 case of Gu Shunzhang (顧順章) is emblematic: after he defected to the KMT, Zhou personally ordered the murder of his entire extended family—over 30 people, including women and children, strangled and buried in a Shanghai garden to avoid the noise of gunshots. This uncompromising ruthlessness was designed to ensure that loyalty within the “United Front” remained unchallenged.⁹

The CCP’s infiltration of the Nationalists was not a side effect but a comprehensive takeover. Agents such as Qian Zhuangfei (錢壯飛) worked at the very heart of the KMT’s intelligence service, forwarding every dispatch to Mao Zedong. Former MIB Deputy Director Weng Yanqing (翁衍慶) describes how the KMT often operated “blind and

⁹ Weng Yanqing (翁衍慶), 中共情報組織與間諜活動, (Engl: *The Communist Party of China Intelligence Organization and Spy*) (Taipei, 2022), pp. 5-7.

deaf” because its own staff was systematically infiltrated by CCP cadres.¹⁰ A clear thread thus runs from the stranglings in Shanghai’s gardens under Zhou Enlai to today’s seamless digital surveillance under Xi Jinping: the CCP does not view Taiwan and the parties there—especially the KMT—as diplomatic partners, but as targets of far-reaching infiltration.

2. The Modern Security Architecture under Xi Jinping

Since Xi Jinping took office, this historically evolved apparatus has been radically centralized under the National Security Commission (中央國家安全委員會), established in 2014. The primary institutional actors—each with massive personnel resources that dwarf any Western intelligence service—are:¹¹

- Ministry of State Security (MSS, 國家安全部): China’s primary civilian foreign intelligence service, responsible for global espionage, counter-foreign influence, and domestic political security. Its Third Bureau conducts operational work specifically targeting Taiwan from a base in Fuzhou/Fujian, exploiting the province’s geographic proximity to the Taiwan Strait. Estimated personnel: 110,000 at headquarters, up to 800,000 across all provincial offices.
- Ministry of Public Security (MPS, 公安部): With approximately 2 million regular police officers, an estimated 300,000 to 500,000 function as a de facto domestic intelligence service. The MPS administers the “Great Firewall,” monitors social media, conducts transnational repression of overseas Chinese communities, and generates vast data that are also used to infiltrate networks abroad.
- People’s Liberation Army – Information Support Force (ISF, 信息支援部隊): Created in April 2024 following the dissolution of the Strategic Support Force (SSF, 戰略支援部隊), the ISF centralizes cyber espionage and SIGINT capabilities. These new units specialize in infiltrating Taiwan’s technological infrastructure and securing information dominance in the event of a conflict.

¹⁰ Weng Yanqing, *The Communist Party of China Intelligence Organization and Spy*, pp. 5-7.

¹¹ Compiled from reports by the Ministry of Justice Investigation Bureau (MJIB), Taipei, 2026; estimates by Taiwanese and international intelligence agencies. Exact figures are classified state secrets.

- United Front Work Department (UFWD, 統一戰線工作部): A political mobilization apparatus coordinating networks of influence through business associations, academic institutions, cultural organizations, and diaspora networks to carry Beijing's interests into the heart of Taiwanese and international civil society.

Beijing has simultaneously transformed decades of operational secrecy into a tightly woven legal framework capable of compelling every Chinese citizen worldwide to cooperate. The National Security Law (2015) asserts sovereignty over Taiwan and defines resistance as a criminal act. The National Intelligence Service Law (2017, Articles 7 and 14) obliges citizens and companies to actively assist in espionage. The Counterespionage Law (2023) permits the detention of any foreigner or Taiwanese citizen on “suspicion”—a practice widely described as “hostage diplomacy.” For Taiwan, this means that any economic exchange with mainland China is a potential vector for infiltration.

3. Taiwan as the Primary Target

The strategic importance of Taiwan for the PRC's security and intelligence policies cannot be overstated. Since 1949, Beijing has regarded Taiwan as an integral part of its national territory, and the collection of political, military, and social intelligence on Taiwan plays a central role across the entire apparatus. The province of Fujian (福建省), geographically proximate to the Taiwan Strait, serves as a key hub for economic and social ties that are simultaneously operational intelligence assets. Officially promoted programs—the Pingtan Comprehensive Pilot Zone, the Kinmen-Xiamen Cross-Strait Integrated Development Demonstration Zone, and various Taiwanese Youth Entrepreneurship Parks—officially pursue economic goals but simultaneously establish institutional networks through which contacts with political and economic elites in Taiwan can be cultivated.¹² According to estimates of intelligence agencies, approximately 180,000

¹² Alex Joske, *Spies and Lies: How China's Greatest Covert Operations Fooled the World* (Melbourne: Hardie Grant, 2022), pp. 45-52.

agents from the PRC's security apparatus work exclusively on the "issue" of Taiwan.¹³

IV. The Power of Numbers: Mass as a Strategic Intelligence Principle

China's intelligence system differs fundamentally from Western services in its organizational logic. While Western services are deliberately kept compact and rely heavily on highly specialized operations, the Chinese system combines professional intelligence organizations with a wide-reaching network of state institutions, party structures, scientific institutions, and economic organizations—what research describes as a "whole-of-society approach."¹⁴ The result is organizational breadth that research consistently identifies as a defining characteristic: the CCP and the PRC cannot function or survive without engaging in massive espionage and the constant surveillance of their own population, without stealing the intellectual property of other countries and systems.

The expression "power of sheer numbers" describes less a precisely measurable quantity than a strategic mindset. While traditional Western intelligence services often rely on a limited number of highly qualified agents, the Chinese system seeks to involve as many individuals and institutions as possible in information-gathering processes. When enough actors simultaneously gather information, establish contacts, and exert influence, a dense network of data, relationships, and opportunities emerges over time. In comparison: the MSS alone employs an estimated 800,000 personnel—against approximately 20,000 for the CIA, 3,500 for MI6, and 6,500 for the BND.¹⁵

This model is particularly effective in the Taiwan context, where economic, cultural, and historical proximity creates numerous legitimate points of contact that

¹³ Background briefing of the author's sources in the PRC and: MJIB, Taipei, 2025. See also: Liu Te-liang (劉德良), "A Brief Discussion on the State of Communist Espionage in Taiwan," *Cross-Strait Situation Analysis Bulletin* (DPP), 2025/8.

¹⁴ Peter Mattis and Matthew Brazil, *Chinese Communist Espionage: An Intelligence Primer* (Annapolis: Naval Institute Press, 2019), pp. 31-40.

¹⁵ Compiled from reports by the Ministry of Justice Investigation Bureau (MJIB), Taipei, 2026; estimates by Taiwanese and international intelligence agencies. Exact figures are classified state secrets.

serve simultaneously as operational opportunities. The semiconductor sector (半導體) has become a primary focus. In 2014, China's State Council published "Guidelines for Promoting the Development of the National Integrated Circuit Industry," establishing a national "Big Fund" (大基金) to recruit semiconductor talent from abroad on a large scale. From 2014 to the end of 2019, approximately 3,000 Taiwanese semiconductor professionals went to mainland China, accounting for 7% of the total workforce in Taiwan's semiconductor industry. After 2019, the trend reversed due to U.S. trade sanctions and technology embargoes against China, combined with significantly improved compensation and prospects at leading Taiwanese firms. As direct talent poaching became more difficult, the CCP shifted to acquiring Taiwanese semiconductor technology through covert capital operations, technical partnerships, scholarships, and supply chain infiltration.

V. The Digital Front: Advanced Persistent Threats (APTs)

In the modern shadow war against Taiwan and Western infrastructure, the line between civilian IT research and state aggression has virtually disappeared. State-controlled hacker groups—Advanced Persistent Threats (APTs)—are firmly embedded in the PRC's power structure, subordinate either to the MSS or to the newly formed ISF. Analysis of 2024–2025 reveals a specialization that goes far beyond mere data theft: it involves the "preparation of the digital battlefield" (戰場準備)—systematic pre-positioning for sabotage operations to be activated in the event of a conflict.

1. Volt Typhoon: Critical Infrastructure Sabotage

Currently regarded as the most dangerous threat to critical infrastructure (KRITIS), Volt Typhoon focuses on systematic infiltration of water utilities, power grids, and transportation systems in the U.S., Guam, and Taiwan. Its defining tactic is "Living off the Land" (LotL): rather than injecting conspicuous malware, the group uses legitimate system tools already present on target computers, making detection extremely difficult. In China, this method is understood as part of "shadow warfare" (影子戰爭). In the

event of a conflict in the Taiwan Strait, these “sleeper accounts” are designed to be activated to paralyze Allied logistics and cause panic among the civilian population through targeted blackouts.¹⁶

2. APT41: Industrial Espionage and Supply Chain Attacks

APT41 (Double Dragon, 雙龍)—affiliated with MSS Offices 10 and 11 in Chengdu—pursues a dual strategy of state espionage and financially motivated cybercrime, an unusual combination that makes it a uniquely versatile threat actor. Its primary focus is the theft of intellectual property in semiconductor technology and biotechnology. Its hallmark tactic is the supply chain attack (供應鏈攻擊): infiltrating software manufacturers to distribute malicious code via official updates to thousands of end users worldwide—a digital Trojan horse in the global supply chain.¹⁷ In August 2019 and September 2020, the U.S. Department of Justice filed charges against individuals linked to the Chengdu 404 Network Technology front company, providing a rare public window into the operation’s structure.

3. RedAlpha / RedJuliatt: Political Intelligence Against Taiwan

Operating out of Fuzhou/Fujian (MSS Office 3), RedJuliatt’s activities are closely linked to United Front work (統一戰線) and focus almost exclusively on the diplomatic and political sphere in Taipei. It targets government agencies, pro-democracy think tanks, and religious organizations through massive phishing campaigns and the creation of deceptively authentic clones of official Taiwanese government login pages.¹⁸ This form of cognitive warfare aims to compromise internal communication channels, steal credentials from key individuals, and spread disinformation through compromised accounts.

¹⁶ Microsoft Threat Intelligence, “Volt Typhoon Targets US Critical Infrastructure with Living-off-the-Land Techniques” (2025/3), visited date: 2026/3/20, 《*Microsoft Security Blog*》, <https://www.microsoft.com/en-us/security/blog/2023/05/24/volt-typhoon-targets-us-critical-infrastructure>.

¹⁷ Mandiant (Google Cloud), *APT41: World War C – The Evolution of a Chinese State-Sponsored Group*, Special Report (2025), pp. 14-19.

¹⁸ Recorded Future (Insikt Group), *RedJuliatt: Targeted Intelligence Collection Operations Against Taiwan*, Research Report (June, 2025).

VI. Methods of Cognitive Warfare and Political Infiltration

1. Disinformation Tactics and the “Inside-Out” Pattern

The CCP's disinformation channels consistently follow an “inside-out” (由內而外) pattern. Narrative themes are established by the party leadership, then mobilized through state and military systems involving a multitude of collaborating organizations, specialized IT companies, marketing firms, and so-called “Internet Water Army Groups” (網路水軍) that systematically spread disinformation at scale. These narratives originate on social media within China (e.g., Weibo), are amplified by content farms and pro-Chinese media abroad, and eventually penetrate mainstream social media and forums in target countries.

The 2018 “Kansai Airport Incident” is a documented example of this playbook deployed against Taiwan: fabricated claims circulated that the Chinese consulate had sent buses to evacuate only Chinese—not Taiwanese—tourists stranded after Typhoon Jebi, deliberately exploiting the politically charged question of Taiwanese identity to create division and alarm.¹⁹ Disinformation campaigns also exploit social fault lines more broadly: exaggerated narratives about “Indian migrant workers” (印度移工) were used to stir conflict and panic within Taiwanese society, demonstrating the CCP's willingness to weaponize any available social tension. Official government documents and news reports are forged to spread unconfirmed rumors such as city lockdowns or mass infections in hospitals. The NSB identified over 4 million suspicious posts in the disinformation category in 2025 alone.²⁰

2. Large-Scale Overseas Propaganda and Media Infiltration

The CCP's “large-scale foreign propaganda” (大外宣) strategy aims to seize “discursive sovereignty” (奪取話語權) over international narratives. Through massive

¹⁹ “Yomiuri Reviews Kansai Airport Incident: Taiwan Faces Fake News Crisis” (2018/10/6), *《Central News Agency (CNA)》*, <https://www.cna.com.tw/news/aopl/201810060004.aspx>; “Chinese Kansai Evacuation Story ‘Fake News’: DPP” (2018/9/9), visited date: 2026/3/12, *《Taipei Times》*, <https://www.taipeitimes.com/News/taiwan/archives/2018/09/09/2003700087>.

²⁰ National Security Bureau (NSB), Republic of China (Taiwan), *Analysis of China's Cognitive Warfare Tactics Against Taiwan in 2025* (2026/1/11), p. 1.

investment in foreign state-run media and the purchase of advertising supplements (such as “China Watch,” 中國觀察) in international mainstream media, the Chinese government’s positive image and viewpoints are promoted as if they were independent editorial content.

At the operational level, journalists are offered all-expenses-paid trips to China; internet celebrities (KOLs, key opinion leaders) are financially supported to create favorable content; and market access and advertising revenue are used to force companies and celebrities into self-censorship (自我審查). Leaked documents from the Chinese cybersecurity firm “I-Soon” (安洵) provided direct evidence of a special “Twitter and public opinion control system” developed to manipulate opinion abroad and suppress dissenting views.²¹ Chinese hacking groups also conduct cyberespionage against foreign governments and companies with the aim of stealing sensitive information—including U.S. trade negotiation strategies and recordings of presidential phone calls—targeting over 80 countries worldwide.

3. Economic Coercion and Its Limits

The CCP uses its enormous economic clout as a strategic tool to punish countries that cross its “political red lines” (政治紅線). Lithuania’s approval of the establishment of a Taiwanese representative office in 2021 prompted the CCP to immediately sever trade ties and exert pressure on multinational companies operating in Lithuania. When Australia called for an investigation into the origins of COVID-19, the CCP imposed high tariffs on numerous Australian goods, resulting in trade losses amounting to billions.

However, a “backfire effect” (反噬效應, boomerang effect) constrains the long-term impact of such measures: countries under pressure actively tap new markets, and the CCP is ultimately forced to lift sanctions due to domestic demand. This demonstrates that the CCP’s economic weapon, while potent in the short term, is not invincible—its effectiveness is constrained by the needs of its own domestic economy. The CCP’s official narrative simultaneously portrays its economic strength as a “contribution to

²¹ Federal Office for the Protection of the Constitution, *BfV Cyber Insight: The i-Soon Leaks – Industrialization of Cyber Espionage* (BFV, 2024/8/1).

globalization,” positioning itself as the “engine of global economic growth” (全球經濟增長的發動機) to obscure the coercive nature of its economic strategy.

4. Political and Social Infiltration

United Front operations abroad recruit community leaders in Taiwan, mobilize “paid demonstrators” (走路工) for political protests, and operate “overseas police stations” (海外警僑驛站) to monitor dissidents, gather information, and intimidate overseas Chinese—constituting “transnational repression” (跨國鎮壓). The Chinese Students and Scholars Association (CSSA, 中國學生學者聯合會) at foreign universities functions as CCP-funded overseas cells that receive instructions from consulates, monitor fellow students, and suppress criticism of China. In Australia, wealthy businesspeople of Chinese descent have reportedly offered donations to major political parties to influence China-friendly policies.²²

Chinese intelligence agencies also target the militaries of other countries, using funds or travel invitations to recruit retired or active-duty military personnel and, in some cases, urging them to “remain passive” (消極不作為) in the event of PLA military actions against Taiwan. Of 159 individuals charged with espionage in Taiwan since 2020, approximately 60% are active or retired military personnel. Particularly alarming are successful infiltrations that extended to the immediate vicinity of the highest state offices, including former assistants to the President, the Speaker of the Legislative Yuan, and advisors to the Office of the President.

VII. The Scope of Espionage: Between 5,000 and 100,000 Agents?

A central point of contention in Taiwan's national security debate is the actual number of Chinese actors on the island. A baseline estimate of 5,000 agents is regarded by experts as a conservative lower limit—first cited by former Deputy Minister of National Defense Lin Chung-pin as early as 2007 and subsequently confirmed as having

²² Clive Hamilton and Mareike Ohlberg, *Hidden Hand: Exposing How the Chinese Communist Party Is Reshaping the World* (London: Oneworld, 2020), p. 112.

been far exceeded by former deputy military intelligence chief Liu Te-liang (劉德良).²³ As early as 2000, the then-deputy director of the NSB, Han Kun (韓岡明 Han Gang-ming), pointed out that among the 540,000 annual visitors from the PRC, at least 3,000 individuals held the status of intelligence operatives.²⁴ Chinese intelligence services operate according to the principle of isolated cells and double coverage, which means that even the adversary cannot provide an absolute total figure.

Primary recruitment channels include social gathering places where contacts are initiated through financial or sexual enticement, organized crime networks, and shell companies. Taiwan's NSB Annual Report for 2025 (published January 2026) documents a massive expansion of cognitive warfare, identifying five key PRC tactics:²⁵ data-driven analysis of Taiwanese social dynamics using big data to tailor narratives for maximum divisive resonance; multi-channel disinformation dissemination across state media, social networks, and local platforms simultaneously to create apparent narrative consistency; AI-powered scaling to produce content in massive quantities; the use of local influencers and collaborative organizations to “localize” narratives and make them appear more credible; and rapid event-hopping, seizing on current crises within hours to reinterpret them in line with PRC interests.

The NSB responded with an integrated reporting and response system: over 3,200 critical disinformation campaigns were reported directly to relevant government agencies in 2025 to enable real-time countermeasures. Taiwan also served as a “frontline state” against cognitive warfare, holding over 80 security dialogues and intelligence conferences with international partners in 2025—including the U.S., the EU, and Australia—to build a “democratic network” for jointly combating information manipulation by totalitarian regimes.²⁶

²³ Background briefing, MJIB, Taipei, 2025. See also Liu Te-liang (劉德良), *Cross-Strait Situation Analysis Bulletin* (DPP, 2025/8), slide “In 2007.”

²⁴ Liu Te-liang (劉德良), “A Brief Discussion on the State of Communist Espionage in Taiwan,” slide “In 2000”.

²⁵ National Security Bureau (NSB), Republic of China (Taiwan), *Analysis of China's Cognitive Warfare Tactics Against Taiwan in 2025* (2026/1/11), p. 1.

²⁶ NSB, *Analysis of China's Cognitive Warfare Tactics Against Taiwan in 2025*, concluding section on international cooperation.

Public opinion data demonstrates that the CCP's operations have, to date, failed in their primary political objective. An opinion poll from April 2025 shows that 84.4% of Taiwanese reject the “One Country, Two Systems” model; 82.5% reject the claim that “Taiwan belongs to China and has never been a state.” The Election Research Center at National Chengchi University documents that the proportion of those identifying as “Taiwanese” remains high, and support for maintaining the status quo or a tendency toward independence is far higher than support for unification.²⁷ This illustrates that the majority of the Taiwanese population continues to view the CCP as unfriendly or hostile—and opposes both military pressure and gray-zone pressure.

VIII. Religious Infiltration: The “Iron Triangle” of Temples, Gangs, and the CCP

The CCP places particular emphasis on Taiwan's cultural and religious identity as a vector for influence operations. The National Security Bureau and international observers note an increasing instrumentalization of the sea goddess Mazu (媽祖), Taiwan's most popular deity. The CCP uses Mazu veneration as “soft power” to construct a shared cultural identity across the Taiwan Strait, subtly presenting “reunification” (統一) as the natural consequence of a shared tradition. Religious practice is thus reinterpreted as a political tool.²⁸

Infiltration occurs through a complex network referred to in expert circles as the “Iron Triangle” (鐵三角): cooperation between Taiwanese organized crime—particularly the Bamboo Union (竹聯幫), one of Taiwan's most powerful criminal organizations with close ties to the mainland—local Mazu temples, and the CCP's United Front Work Department. This alliance enables Beijing to exert influence deep into the local structures of Taiwanese society that are often difficult for state security agencies to reach.²⁹

²⁷ Mainland Affairs Council (MAC), “Opinion Poll” (2025/4/24), visited date: 2025/12/31, *《Mainland Affairs Council》*, <https://www.mac.gov.tw>.

²⁸ Religioscope Institute, *Mazu, Political Influence and Organized Crime in Taiwan*, Papers on Contemporary Religion (Fribourg, April, 2025), Chapter 3, pp. 21-43.

²⁹ Religioscope Institute, *Mazu, Political Influence and Organized Crime in Taiwan*, pp. 21-43.

A prominent example of institutional influence is the Dajia Jenn Lann Temple (大甲鎮瀾宮). By controlling influential religious institutions, the United Front shapes the discourse during major Mazu pilgrimages that mobilize millions of people. These events are used to promote cross-strait exchange programs in which Taiwanese believers on the mainland are deliberately exposed to CCP political messages. Organizations such as the Taiwan Mazu Fellowship Association function de facto as United Front channels, coordinating hundreds of temples in Taiwan with their “mother temples” in China (particularly on the island of Meizhou in the Fujian province) to establish a permanent flow of influence. Temple financial flows also provide opportunities to circumvent financial controls and launder money to finance political activities—with the gangs’ criminal networks handling the logistics.

The danger of this “religious infiltration” lies in its subtlety. Since religious freedom is a cherished value in Taiwanese democracy, government authorities often hesitate to intervene in temple affairs, creating a safe space in which United Front operations proceed largely unhindered. In the event of a conflict, these networks could be activated to incite social unrest, carry out acts of sabotage, or hinder military mobilization.

IX. The Political Turn of 2025: President Lai’s Security Agenda

For a long time, it seemed as though the Taiwanese government was not confronting hybrid threats with the necessary resolve. Critics such as former intelligence chief Liu Te-liang pointed out that “treason was sometimes punished more leniently than the theft of a washing machine,” and that existing laws—including the Anti-Infiltration Act (反滲透法)—were too narrowly defined to counter modern influence operations carried out through front companies and online networks. This changed fundamentally in 2025 when President Lai Ching-te (賴清德) declared national security a top priority.³⁰

³⁰ “Taiwan Reports Significant Rise in Suspected Chinese Espionage” (2025/1/13), visited date: 2026/2/1, *《Reuters》*, <https://www.reuters.com/world/asia-pacific/taiwan-reports-significant-rise-suspected-chinese-espionage-2025-01-13/>.

Following a meeting of the high-level National Security Council, President Lai delivered a keynote address on 2025/3/13, that is regarded as a strategic milestone for the defense of Taiwanese democracy. Lai issued a stark warning about how Chinese state media uses narratives to stir up internal opposition, with individuals literally making careers out of producing United Front content. He quoted Professor Kerry K. Gershaneck on China's plan to “divide and conquer us through subversion, infiltration, and the acquisition of media outlets, as well as by launching media warfare, psychological warfare, and legal warfare.”³¹

The speech represented a significant legal and political shift: the first time a Taiwanese government official officially designated China as a “foreign hostile force” under the Anti-Infiltration Act. Lai stated: “By its actions, China already meets the definition of a ‘foreign hostile force’ as provided in the Anti-Infiltration Act. We have no choice but to take even more proactive measures ... It is time we adopt proper preventive measures, enhance our democratic resilience and national security, and protect our cherished free and democratic way of life.”³²

Lai also cited concrete examples of Chinese infiltration: targeted influence operations and recruitment of active and former military personnel; systematic influence on media outlets, political commentators, and artists; the use of Chinese state media combined with co-opted local actors to disseminate divisive information; and identity-based manipulation using economic and social inducements to confuse the national identity of Taiwanese people.

In September 2025, Lai stepped up the pace, announcing a massive wave of legislation: based on 17 national security strategies, over a hundred legislative amendments were introduced. The “Four Key Elements for Protecting Taiwan” were defined as: cultural identity (文化認同), democratic institutions (民主體制), economic strength (經濟實力), and sound social systems (健全社會制度). Despite

³¹ Office of the President, Republic of China (Taiwan), “President Lai Holds Press Conference Following High-Level National Security Meeting” (2025/3/13), visited date: 2026/2/13, *Office of the President, Republic of China (Taiwan)*》, <https://www.president.gov.tw>.

³² Office of the President, Republic of China (Taiwan), “President Lai Holds Press Conference Following High-Level National Security Meeting”.

the announced reforms, the KMT and the Taiwan People's Party (TPP) used their majority in the Legislative Yuan to block key defense budgets, including the special defense budget of 1.25 trillion NT\$, in the procedural committee.

X. Strategic Paralysis: The “Fifth Column” and Parliamentary Stability

What may appear on the surface to be lively democratic discourse is, upon closer analysis, a coordinated strategy of destabilization. The goal of this “fifth column” is no longer merely traditional espionage but the institutional paralysis of the state from within. The Legislative Yuan has become a central arena for this destabilization: the TPP, under its caucus leader Huang Kuo-chang (黃國昌), introduced its own defense budget draft that, according to Ministry of National Defense experts, is strategically flawed and deliberately omits essential elements of U.S. cooperation—including software for tactical networks and spare parts for helicopters.³³ This selective budgeting jeopardizes the sustainability of Taiwan's combat readiness and hinders joint operations with allies.

Renowned China expert Willy Lam (林和立) offers a stark assessment: “The KMT will not resist any kind of occupation of Taiwan by China. Much of the party seems already controlled by the CCP,” he says. The KMT is no longer viewed by Beijing merely as a political partner, but as a faction whose leadership is de facto under the financial and ideological control of the Chinese Communist Party. There is a widespread view that the KMT has essentially been ‘bought’ to politically neutralize Taiwan from within.”³⁴ The KMT's new chairwoman, Cheng Liwen (鄭麗文), has advanced decidedly pro-China narratives that increasingly call Taiwan's sovereignty into question,

³³ Jamestown Foundation, “China's United Front Work in Taiwan: A 2025 Assessment,” *China Brief* (Washington, D.C., 2025), pp. 12-18.

³⁴ Willy Lam (林和立), remarks at the Taiwan Foreign Correspondents' Club (TFCC); email exchange with the author, 2025/9/1. See also Jürgen Kremb, “Chinas Angriff auf Taiwan hat längst begonnen” (2026/2/25), *WirtschaftsWoche*, <https://www.wiwo.de/politik/ausland/taiwan-chinas-angriff-auf-das-land-hat-laengst-begonnen/100203395.html>.

flanked by Parliament Speaker Han Kuo-yu (韓國瑜), who has drawn controversy due to his closeness to representatives of the Beijing Liaison Office in Hong Kong.

Personnel infiltration has also reached the parliamentary level. The TPP's attempt to bring Lee Chen-hsiu (李貞秀)—born in China and having not officially renounced PRC citizenship—into parliament raises significant constitutional questions, since law prohibits individuals with dual citizenship from holding high public office. The broader phenomenon of “Zhongpai” (中配 —Chinese wives of Taiwanese citizens deliberately exploited as agents of influence) exemplifies how social infiltration complements political and military espionage.³⁵ The Jamestown Foundation's 2025 assessment of United Front activities confirms that Beijing has intensified efforts not only to co-opt elites but also to directly influence Taiwanese civil society through social media and migrant networks, aiming to undermine the government's ability to govern by creating “chaos from within.”³⁶

XI. Geopolitical Escalation: The “Japan Crisis” of Late 2025

In late 2025, the CCP massively expanded its hybrid warfare arsenal to target Japan following a statement by Japanese Prime Minister Sanae Takaichi (高市早苗) during a session of the House of Representatives on 2025/11/7, officially designating a potential “Taiwan incident” (臺灣有事) as an “existential crisis situation” (存立危機事態) for Japan.³⁷ Beijing's reaction was immediate and unusually sharp: Chinese Consul General in Osaka Xue Jian (薛劍) posted remarks on Twitter calling for “filthy heads that dare to intrude without permission” to be “cut off without hesitation”—a

³⁵ “Chinese Spouse Faces Scrutiny before Joining Taiwan Legislature” (2024/11/8), *《Taiwan News》*, <https://www.taiwannews.com.tw/news/5967732>; see also Taipei Times, “Red Bloggers Deported for Spreading Pro-China Propaganda” (2025/4/8), *《Taipei Times》*, <https://www.taipeitimes.com/News/taiwan/archives/2025/04/08/2003834814>.

³⁶ Jamestown Foundation, “China's United Front Work in Taiwan: A 2025 Assessment,” pp. 12-18.

³⁷ IORG (Taiwan Information Environment Research Center), Weekly Report No. 128: “The CCP's Complex Threats Against Japan” (2025/12/29), visited date: 2026/1/10, *《IORG》*, <https://iorg.tw>.

statement that caused worldwide outrage.³⁸

Starting in mid-November 2025, the CCP launched a coordinated campaign encompassing cognitive, diplomatic, military, and economic dimensions: state-run media published a series of statements culminating in a People's Daily editorial declaring Takaichi's "provocative transgression" would not be tolerated; Beijing issued travel warnings for Japan, announced naval exercises in the Yellow Sea, and completely halted imports of Japanese seafood on November 19. Even panda diplomacy was exploited, with Chinese media declaring the early return of pandas from Tokyo's Ueno Zoo in December 2025 to be the end of an era.³⁹

Particularly concerning, according to the Taiwan Information Environment Research Center (IORG), was the increasing synchronization of narratives between the CCP and the Taiwanese opposition parties, the KMT and TPP. Within the Chinese-language information space, these actors jointly shaped an alternative worldview: deliberately emphasizing Japan's wartime history and using terms such as "Nazi", "militarism" (軍國主義), "far-right," and "warmongering" to discredit Prime Minister Takaichi and President Lai Ching-te. KMT figures including Ma Ying-jeou (馬英九), Hung Hsiu-chu (洪秀柱), and Kao Chin-su-mei (高金素梅) made statements—such as that the Taiwan Strait "is none of the Japanese's business"—that de facto undermined the Republic of China's international position and echoed Beijing's false premise that the Strait is purely China's internal matter.⁴⁰

XII. Espionage Cases and Legal Consequences (2025–2026)

The year 2025 marked a turning point in Taiwanese legal history. Faced with a

³⁸ IORG (Taiwan Information Environment Research Center), Weekly Report No. 128: "The CCP's Complex Threats Against Japan". Original text of Xue's post: "那種擅自闖入的骯髒頭顱，就應該毫不猶豫斬掉。你們做好覺悟了嗎？"

³⁹ IORG (Taiwan Information Environment Research Center), Weekly Report No. 128: "The CCP's Complex Threats Against Japan".

⁴⁰ IORG Weekly Report No. 128: Statements by Ma Ying-jeou (馬英九), Hung Hsiu-chu (洪秀柱), and Kao Chin-su-mei (高金素梅). See also: IORG Monthly Report, December 2025, section "Division of Labor in U.S. Discourse."

massive increase in investigations—case numbers rising steadily since 2022, with active and former military personnel accounting for approximately 66% of espionage cases—the government ended the era of lenient sentences through consistent application of the reformed National Security Act. Efforts to reestablish special military courts are also being pursued. Selected final convictions include:⁴¹

- Rehabilitation Alliance Party chairman Qu Hongyi (屈宏義): 10 years, January 2026. He had recruited retired officers on behalf of the PLA to form an “internal force” and transmit strategic coordinates, including those from the American Institute in Taiwan (AIT).
- Three former members of the Presidential Office Security Unit: up to 7 years, December 2025, for passing sensitive information to China.
- Former Air Force officer Shih Chun-cheng (史濬程): 2 years and 2 months, August 2025, for National Security Act violations.
- Four former DPP officials: 4 to 10 years, September 2025, for passing government leaders’ travel itineraries to Beijing. Huang Chu-jung received the maximum sentence of 10 years.
- Diabolo coach Lu Chi-hsien (魯紀賢): 10 years and 6 months, June 2025, for building an extensive network recruiting military and coast guard officers.
- Former NSB agent Peng Shun-fu (彭順富): 4 years, definitively sentenced by Taiwan’s Supreme Court, 2026/3/11.

Among ongoing cases, the Ting Hsiao-hu network (November 2025) involves seven individuals charged with establishing a network under the guise of business trips that paid over 11 million NT\$ in bribes to active and retired officers. A reserve captain was indicted in November 2025 for selling military secrets via Telegram. A journalist was detained in January 2026 suspected of acting as an intermediary to bribe military

⁴¹ “Supreme Court upholds sentences given to pro-China campaigners” (2026/1/29), *《Central News Agency (CNA)》*, <https://focustaiwan.tw/cross-strait/202601290009>; “Supreme Court finalizes ex-servicemen spying case with maximum 7-year term” (2025/12/5), *《Focus Taiwan》*, <https://focustaiwan.tw/cross-strait/202512050012>; “Four former DPP aides sentenced for espionage” (2025/9/26), *《AP News》*, <https://www.taipeitimes.com/News/taiwan/archives/2025/09/26/2003844457>; “Diabolo Instructor and His Spy Ring Sentenced to Jail” (2025/7/1), *《Taipei Times》*, <https://www.taipeitimes.com/News/taiwan/archives/2025/07/01/2003839548>.

personnel into disclosing classified information.

The legal framework applied rests on four pillars: the National Security Act (國家安全法) as the core instrument against hostile organizations and espionage; the Classified National Security Information Protection Act (國家機密保護法) for the betrayal of state secrets by public officials; the Anti-Infiltration Act (反滲透法) for cases of illegal political influence through foreign funds; and the Criminal Code of the Armed Forces (陸海空軍刑法) imposing stricter penalties for soldiers who betray military secrets.⁴²

XIII. Strategic Recommendations: The Defensible Republic

Taiwan's role as a “canary in the coal mine” of global freedom cannot be overstated. Just as birds in mines once provided early warning of odorless, deadly gases, the intensity of Chinese operations against Taipei signals the harbingers of a global threat. The methods tested here—from the exploitation of economic dependencies to cognitive warfare and the covert infiltration of spies and collaborators—serve as blueprints for future operations against Europe and North America. The following recommendations therefore address both the government in Taipei and European security agencies and political institutions.

1. Legal Reform: From Procedural to Robust Rule of Law

It is a security policy absurdity when treason and espionage are punished more leniently than ordinary property crimes. Particularly serious cases—the disclosure of strategic defense plans or active sabotage of national defense capabilities—should be punishable by life imprisonment even in peacetime. Robust emergency legislation modeled on the German Emergency Laws should authorize the executive to make central security policy decisions by decree if the legislature becomes incapacitated due to infiltration or targeted obstruction. A state that loses its ability to act in the face of

⁴² Anti-Infiltration Act (反滲透法), promulgated 2020/1/15; Classified National Security Information Protection Act (國家機密保護法), last amended 2023/12/27; National Security Act (國家安全法); Criminal Code of the Armed Forces (陸海空軍刑法). All available at the *《Laws and Regulations Database of the Republic of China (Taiwan)》*, <https://law.moj.gov.tw>.

infiltration brings about its own downfall—what philosophers have called Popper's Paradox of Tolerance applied to democratic institutions.

2. Societal Defense and Asymmetric Resilience

Military deterrence against the PRC remains indispensable, but it is incomplete without societal resilience. The population must be comprehensively prepared for the reality of asymmetric conflict and civil resistance. This includes the decentralization of defense structures and psychological mobilization: every citizen should be aware that the country is infiltrated by agents—in religious organizations, business associations, and social networks. Financial flows of religious organizations, elected officials, and Taiwanese businesspeople with PRC connections must be monitored without exception. Vigilance against infiltration attempts must be enshrined as a national civic duty.

3. The Cognitive Firewall: Education and Media

The fight against infiltration begins in the minds of the people. The education system must be understood as a strategic defensive weapon: the history of the CCP—from the “Great Leap Forward” and the “Cultural Revolution” through the Tiananmen Square massacre to the ongoing repression in Tibet, Xinjiang, and Hong Kong—must be embedded in the curriculum in its full, unvarnished reality. Only those who understand the nature of totalitarian rule in Beijing are immune to the promises of United Front propaganda. Civil resistance, guerilla warfare and crisis management should become part of school education to strengthen societal self-organization under pressure.

The media landscape must simultaneously undergo critical review. Freedom of the press must not be abused as a license for cognitive sabotage. Journalists, media outlets, and social media influencers who demonstrably act as multipliers of externally controlled disinformation must be held personally and institutionally liable. Analogous to the ban on Nazi propaganda and Holocaust denial in Germany and Austria, legislation prohibiting the promotion of CCP narratives or incitement to aggression against Taiwan should be passed by the Legislative Yuan. A ban on TikTok and similarly manipulative platforms, analogous to Australia's approach, would significantly curb Beijing's

cognitive warfare capabilities.

4. Parliamentary Integrity and the “Fifth Column”

The Legislative Yuan must be restored as a place of national dignity and sovereignty. Actors within political parties whose actions systematically advance Beijing’s strategic interests must undergo thorough security screening. In cases of proven collaboration with or funding by United Front bodies, the loss of parliamentary seats, revocation of immunity, and criminal prosecution should be possible. Travel by elected officials to China must be prohibited until Beijing has signed a non-aggression pact with the ROC—a measure that should also apply to representatives of municipal councils and local authorities given the level of penetration documented in this study.

5. International Intelligence Alliance and European Responsibility

Defending against modern espionage is a transnational task. Taiwan possesses insights into the methods of Chinese intelligence services that are unique worldwide. This knowledge is a strategic asset that should not remain confined to bilateral arrangements. European services—including Germany’s BND and BfV, the British MI6, and the CIA—should massively intensify strategic exchange and cooperative engagement with Taiwan’s security apparatus. Taiwan must not be left out as a senior partner in the field of China expertise. In return, Europe should provide Taiwan with technological support for cyber defense and the protection of critical infrastructure. European states should use Taiwan’s infiltration patterns as a benchmark to identify their own fifth columns in domestic parliaments at an early stage. Anyone who wants to understand how Beijing exerts influence in Berlin or Brussels must study operations in Taipei.

6. Strategic Vision: Post-Xi Jinping Diplomacy

Despite the need for firmness, Taiwan must demonstrate strategic foresight and keep the door open for a future beyond the Xi Jinping era. A wise strategy combines a resolute defense posture with keeping diplomatic options open. The “one country, two

systems” model has proven definitively unworkable, as Hong Kong’s experience since 1997 has demonstrated. A confederal arrangement, a non-aggression pact backed by binding mutual defense guarantees from Washington and democratic Asian neighbors, and the internationalization of the conflict—for example through UN-facilitated talks at UN offices in Vienna—are scenarios worth developing. The admission of Taiwan into the UN or other international organizations, following the precedent by which Ukraine and Belarus held separate seats in the UN General Assembly in the USSR-era, could serve as a model. Such signals indicate to the international community that Taiwan seeks not confrontation but a stable order based on freedom and democratic self-determination.

XIV. Conclusion

The study concludes that the infiltration of Taiwan is not a local problem but a global warning sign. The methods Beijing is perfecting in Taiwan—the combination of high-tech espionage, economic blackmail, and psychological manipulation—are already being used worldwide against Western democracies. Europe and the United States must view Taiwan not only as a partner in chip production but as a leading expert in countering hybrid threats. Taiwan’s defense hinges on its ability to identify internal enemies and strengthen national resilience. Only a resilient democracy prepared to fight its enemies with the necessary resolve while simultaneously formulating a clear vision for the future will be able to withstand the PRC’s total infiltration. Taiwan is the bulwark of freedom in Asia—if this bulwark falls, freedom worldwide will be at stake.