



**FRIEDRICH NAUMANN
FOUNDATION** For Freedom.

Taiwan / Global Innovation Hub

POLICY PAPER

THE WAR OF SPIES

**How China's Intelligence Services Are Infiltrating
Taiwan—and What Europe Must Learn from It**

Jürgen Kremb

Publication Credits

Publisher

Taiwan Office/ Global Innovation Hub
Friedrich Naumann Foundation for Freedom
15F.-6, No. 171, Songde Road,
Xinyi District, Taipei City 110030
Taiwan

 freiheit.org/Taiwan

 FNFGIHUB

 FNFreiheit

 FNFGIHUB

Author

Jürgen Kremb, Journalist, Author
and Sinologist; Taiwan Fellow 2025;
Visiting Scholar, Human Rights Institute,
Soochow University, Taipei

Editor

Taiwan Office/Global Innovation Hub,
Friedrich Naumann Foundation
for Freedom

Contact

A security policy study as part
of the **Taiwan Fellowship 2025**



(c) MOFA, Taiwan

Phone +886 2 2728 1500

Email globalinnovation@freiheit.org

Date

September 2026

Notes on using this publication

This publication is an information offer of the Friedrich Naumann Foundation for Freedom. It is available free of charge and not intended for sale. It may not be used by parties or election workers for the purpose of election advertising during election campaigns (federal, state or local government elections, or European Parliament elections).

License

Creative Commons (CC BY-NC-ND 4.0)

Table of Contents

Summary of the Study: The War of Spies – How China’s Intelligence Services Are Infiltrating Taiwan	7
The Conceptual Framework	7
The Architecture of Infiltration: The Legacy of the United Front	7
The Intelligence Octopus: MSS and the New Role of the PLA	7
Methods of Subversion: Bribery, Blackmail, and Disinformation	8
Cyberspace and the Cognitive Firewall	8
The Defensible Republic: Taiwan’s Response to the Threat	8
Conclusion and Global Implications	8
Key Insights at a Glance	9
Research Approach	10
Chapter 1 – Introduction: Why Focus on Chinese Espionage? China’s Strategy Toward Taiwan in Light of Geopolitical and Psychological Paradoxes	11
Chapter 2 – In the Eye of the Storm: The Academic Debate on Cognitive Warfare and Hybrid Threats	14
2.1. Cognitive Warfare: Beyond FIMI	14
2.2. The United Front: Instrumentality Rather Than Friendship	15
2.3. Hybrid Warfare and the Gray Zone	15
2.4. The Interaction of Spheres	16
2.5. Conclusion: Synergy of Destabilization	16
Chapter 3 – The Architecture of the “Secret Front.” The Genesis of Chinese Intelligence Services versus the KMT and Taiwan.	17
3.1. The Era of the “Red Brigade”: Zhou Enlai and the Professionalization of Terror	17
3.2. The “Magic Weapon”: The United Front (統一戰線)	17
3.3. Intelligence Agencies in Mao Zedong’s Red People’s Republic	18
3.4. Institutional Structure and the “Xi Revolution”	18
3.5. The New Legal Landscape: Espionage as a Civic Duty	19
3.6. Conclusion: The Continuity of Violence	20

Chapter 4 – The Power of Sheer Numbers. Personnel and Structures	21
4.1. Numbers Matter	21
4.2. At the Heart of the Surveillance Apparatus – The MSS	24
4.3. The Ministry of Public Security (MPS)	26
4.4. Military Intelligence Services and Information Warfare	26
4.5. Social Networks as Multipliers	26
4.6. Taiwan as a Key Target of Chinese Intelligence Activities	26
Chapter 5 – Shadows on the Net. The Role of Advanced Persistent Threats (APTs)	28
5.1. Volt Typhoon: Sabotage of Critical Infrastructure (MSS/PLA – Hybrid)	28
5.2. APT41 (Affiliated with: MSS – Office 10/11 in Chengdu/Sichuan)	28
5.3. RedAlpha / RedJuliett (Affiliated with: MSS – Bureau 4 in Fuzhou/Fujian)	30
Chapter 6 – The Facets of the CCP's Cognitive Warfare in Democratic Countries, Including Taiwan.	31
6.1. Background	31
6.2. Methods of Information and Cognitive Warfare (資訊與認知戰)	33
6.3. The Actors of Political and Social Infiltration (政治與社會滲透)	36
6.4. The Challenges for Taiwan (對臺灣的挑戰)	37
6.5. In Background Discussions, Taiwan's Security Agencies Have Summarized the Following Demands based on This Analysis	38
6.6. The Security Organs of the CCP, Assessment and Classification regarding Threats to Regional, Asian, and International Security. Classification of Leaders	38
6.7. What are the Main Targets of the Chinese Security Agencies ...	43
6.8. Structure of the CCP's Working System for Propaganda Directed at Taiwan and Abroad	46
Chapter 7 – Analysis of Chinese Espionage Activities. Have 5,000 or 100,000 Chinese Agents Infiltrated Taiwan?	52
7.1. Definition and Distinction: United Front vs. Espionage	52
7.2. The Debate Over Quantifying Infiltration	52
7.3. Analysis of Cognitive Warfare: The NSB Annual Report 2025	53
7.4. Response Mechanisms and International Cooperation	54
7.5. The Economics of Espionage and Conclusion	54

Chapter 8 – Religious Infiltration and the “Iron Triangle” – The Instrumentalization of Mazu Worship and Organized Crime	55
8.1. The United Front and the “Soft Power” of the Sea Goddess	55
8.2. The “Iron Triangle”: Temples, Gangs, and the CCP	55
8.3. The Role of Organized Crime: The Bamboo Union	55
8.4. Institutional Hijacking: The Case of the Dajia Jenn Lann Temple	55
8.5. The “Taiwan Mazu Fellowship Association” as a Network	56
8.6. Financial Dependencies and Money Laundering	56
8.7. The Tianjin Binhai Mazu Cultural Park	56
8.8. Threat to the Substance of Democracy	56
8.9. Security Implications	56
8.10. Summary: The Need for a Holistic Defense	56
Chapter 9 – The Political Turn of 2025: President Lai’s Security Agenda and the New Wave of Legislation	57
9.1. From Restraint to a Defensive Democracy	57
9.2. The President’s Speech as a Milestone (March 13, 2025)	57
9.3. Appeal to the Population and Civil Resilience	58
9.4. The Opposition’s Response: Criticism and Obstruction	59
9.5. The Legislative Offensive (September 2025)	59
9.6. Conclusion	59
Chapter 10 – Strategic Paralysis: The “Fifth Column” and the Erosion of Parliamentary Stability	60
10.1. The Artificial Crisis	60
10.2. The Parliamentary Blockade: Defense in the Crosshairs	60
10.3. The Role of the KMT and Willy Lam’s Analysis	60
10.4. Radicalization in Personnel Policy: Cheng Li-wun and Han Kuo-yu	61
10.5. Personnel Infiltration: The Case of Lee Chen-hsiu and the “Zhongpai”	61
10.6. The United Front Network: The Jamestown Analysis	61
10.7. Conclusion	61

Chapter 11 – The “Japan Crisis” – Geopolitical Escalation and Cognitive Synchronization	62
11.1. The “Taiwan Incident” as an Existential Crisis	62
11.2. Hybrid Threats: The Multidimensional Escalation	62
11.3. Cognitive Synchronization: The Alliance of Narratives	62
11.4. Defamation of the Lai Administration	63
11.5. Conclusion	63
Chapter 12 – Specific Espionage Cases and Their Criminal Consequences	64
12.1. The Judiciary in the Fight Against Infiltration (2025–2026)	64
12.2. Final Convictions (Spies and Collaborators)	64
12.3. Ongoing Charges and Suspected Espionage Cases (as of March 2026)	65
12.4. Summary Analysis of the Legal Basis	65
12.5. Bibliography (Court Decisions & Primary Sources)	66
Chapter 13 – Strategic Recommendations: The Defensible Republic	67
13.1. Introduction: Taiwan as the “Canary in the Coal Mine”	67
13.2. Paradigm Shift in Criminal Law: From Procedure to Resilience	67
13.3. Physical Security and Operational Lessons: The Case of Puma Shen	68
13.4. Society-wide Defense and Asymmetric Resilience	68
13.5. The Cognitive Firewall: Education and Media as Defensive Weapons	69
13.6. Parliamentary Integrity and the “Fifth Column”	70
13.7. International Intelligence Alliance and European Responsibility	70
13.8. The Post-Xi Jinping Era. Diplomatic Creativity Versus Confrontation.	71
13.9. Final Assessment	72
Acknowledgments	73
Glossary	75
Current Overview of Leadership Roles in the PRC’s Intelligence and Security Services <i>(as of March 2026)</i>	80
Footnotes and Notes on the Text	82
Index of Names	94
About the Author	98

Summary of the Study: The War of Spies – How China's Intelligence Services Are Infiltrating Taiwan

The Conceptual Framework

Taiwan as a Laboratory for Cognitive Warfare. **The study posits that Taiwan is far more than just a territorial target for the People's Republic of China (PRC); it serves as a global testing ground for a new form of conflict known as "cognitive warfare."** Unlike traditional espionage, this strategy aims to manipulate the consciousness, perceptions, and ultimately the decision-making behavior of Taiwanese society as a whole. In doing so, the PRC combines traditional intelligence methods with modern psychological operations to destabilize Taiwan from within without firing a single shot. **This "comprehensive operation" exploits the openness of Taiwanese democracy as a gateway to sow distrust in state institutions and undermine social cohesion.**

The Architecture of Infiltration: The Legacy of the United Front

A central element of the Chinese strategy is the so-called United Front work. Historically rooted in the struggle against the KMT, this instrument has, according to analysts, evolved into a highly efficient power machine under **Xi Jinping** (习近平). **The United Front does not operate in secret like a classic intelligence service, but rather utilizes organizations, business associations,**

and cultural societies that operate openly or semi-openly. Its goal is the "instrumentalization of friendship": by co-opting elites from politics, business, and religion, a network is created that carries Beijing's interests into the heart of Taiwanese society. The line between legitimate political influence and illegal covert operations is becoming increasingly blurred.

The Intelligence Octopus: MSS and the New Role of the PLA

The operational burden of infiltration rests on several pillars. **The Ministry of State Security (MSS) serves as the primary actor for civilian foreign intelligence and the recruitment of informants within the Taiwanese administration.** This is supported by the *Ministry of Public Security (MPS)*, which monitors the diaspora and social movements.

The recent restructuring of the *People's Liberation Army (PLA)* represents a radical turning point. With the dissolution of the *Strategic Support Force (SSF)* and the creation of the *Information Support Force (ISF)* in April 2024, Beijing has centralized its capabilities in the areas of cyber espionage and SIGINT (electronic intelligence). **These new units specialize in infiltrating Taiwan's technological infrastructure and securing information dominance in the event of a conflict.**

Methods of Subversion: Bribery, Blackmail, and Disinformation

The study identifies a wide range of infiltration methods. “Economic dependence as a weapon” has proven particularly effective. **Through the so-called Taishang—Taiwanese businesspeople with massive investments on the mainland, Beijing exerts direct political pressure on Taipei. In the military sphere, the analysis reveals an alarming number of espionage cases in which active and former officers of the Taiwanese armed forces were recruited for information on U.S. weapons systems or defense plans.** Often, the initial contact begins innocently via social networks such as Telegram or LinkedIn and leads to long-term espionage relationships through targeted bribery or the exploitation of personal vulnerabilities.

Cyberspace and the Cognitive Firewall

In the digital realm, China is waging a constant war of attrition. Every day, Taiwan is exposed to millions of cyberattacks carried out by state-sponsored hacking groups (APTs, Advanced Persistent Threat). These operations serve not only to steal data but also to prepare disinformation campaigns. Artificial intelligence is increasingly being used to produce deceptively realistic deepfakes designed to exacerbate political tensions. **The study highlights that Taiwan’s technological superiority in the semiconductor industry simultaneously represents**

an enormous vulnerability, as industrial espionage aims to undermine the country’s economic foundation.

The Defensible Republic: Taiwan’s Response to the Threat

Taiwan has responded to these existential challenges by strengthening its security architecture. The Anti-Infiltration Act and the reform of national security laws form the legal framework for punishing covert influence by “hostile external forces.” However, the study emphasizes that purely state-led measures are insufficient. **The true line of defense lies in societal resilience. Initiatives to strengthen media literacy and cooperation between the government and civil society (e.g., through fact-checking organizations) are central to maintaining the cognitive firewall against Chinese disinformation.**

Conclusion and Global Implications

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 U.S. must view Taiwan not only as a partner in chip production but as a leading expert in countering hybrid threats.** The fate of Taiwanese democracy will depend on whether it succeeds in neutralizing the “fifth column” within its borders while

simultaneously intensifying international intelligence cooperation. Taiwan is the canary in the coal mine of global freedom; its silence would be a harbinger of a far greater catastrophe.

Key Insights at a Glance

- **The Hybrid Mix:** China no longer distinguishes between peace and war, but operates in a permanent gray zone where information is the most important weapon.
- **Mass of Personnel:** The sheer number of actors involved (MSS, MPS, ISF, United Front) overwhelms traditional defense mechanisms with a flood of simultaneous operations.
- **Legal Aggression:** The PRC has elevated espionage to a civic duty through “national security” laws, making any contact with the mainland a potential security risk for Taiwanese citizens.
- **International Alliance:** Without an institutionalized exchange of intelligence between Taiwan and the West, the defense remains incomplete.
- **Civil Defense:** Taiwan’s future hinges on its ability to identify internal enemies and strengthen national resilience. Only a strong democracy, prepared to fight its enemies with the necessary resolve, can succeed. **Taiwan is the bulwark of freedom in Asia—if this bulwark falls, freedom worldwide will be at stake.**

Research Approach

This study examines the PRC's systematic preparations for a potential conflict with Taiwan and, beyond that, with Western democracies. To this end, it analyzes how Chinese security and intelligence services influence, infiltrate, and destabilize Taiwan's strategic, psychological, and social landscape. The central question is how classic intelligence operations, united front work, cognitive warfare, and hybrid influence strategies combine to form a comprehensive "overall operation" by China that goes far beyond traditional espionage activities.

The analysis is based on a combination of academic literature, primary sources, reports from Taiwanese security agencies, international think tank studies, and background discussions with experts

from intelligence services and government institutions of the *Republic of China* (ROC) in Taiwan. The goal is to develop an integrated understanding of the threat landscape and to offer concrete recommendations for action to both Taiwan and Western actors.

The central thesis is that Taiwan serves as the "laboratory" for Chinese influence operations in the 21st century. The methods Beijing is testing in Taiwan serve as a model for global application against democratic states, particularly in Europe and the United States. Taiwan is thus not only a stage but also a testing ground for a new form of political-strategic confrontation, the primary goal of which is not military conquest but the psychological paralysis of the adversary.

Chapter 1 – Introduction:

Why Focus on Chinese Espionage?

China's Strategy Toward Taiwan in Light of Geopolitical and Psychological Paradoxes

I am a journalist and have spent much of my adult life in East and Southeast Asia. After studying Chinese in Taiwan, I lived in Beijing for eight years as bureau chief of the German news magazine *DER SPIEGEL* (1990–98). Subsequently, with a brief interruption in Vienna, I reported intensively for a good two decades on terrorism, Islamism, and the work of Asian security services from Singapore (1998–2024).¹

In the People's Republic of China in particular, surveillance, obstruction, and threats—even active intimidation by secret and security services—are part of everyday life, especially for media representatives, but also for all foreigners in the country.²

That this is not a new phenomenon is illustrated by the following incident from the early 1990s, which I experienced firsthand. It should be noted that this case study is not unique; rather, many colleagues who reported from China at the time have similar stories to tell: ³

I had just settled into my correspondent post in Beijing when I set off with my family for a vacation at the home of a Swiss diplomat. The residence was located at the end of a secluded side valley near the Alpine village of Engelberg. On the first

morning of our vacation, we were sitting on the balcony having breakfast when a limousine with a license plate from the Chinese Embassy in Bern pulled up in front of the property. Immediately afterward, four men wearing sunglasses got out, spoke to each other in a northern Chinese dialect, and took conspicuously obvious photos of me and the entire family. After about ten minutes, they got back into the car and drove away. A call to the security officer at the German Embassy in Beijing to inquire about the possible meaning of such an action yielded the following response: “That was intended as an intimidation tactic by the Chinese security services. It’s meant to make it clear that we always know where you are and what you’re doing.”

Similar incidents recurred throughout the entire duration of my work in China. Until that day in November 1998, when eight intelligence agents stormed my office in the Qijiyuan complex in Beijing’s diplomatic quarter, searched the rooms for alleged “secret government documents,” and I was officially expelled from the country two days later.⁴

Taiwan’s intelligence services are highly valued in the West for their specific

knowledge of China. It is no coincidence that the *foreign intelligence service of the Federal Republic of Germany (Bundesnachrichtendienst, BND)* has maintained close cooperation since the early 1960s with the *National Security Bureau (NSB, 國家安全局)* in Taipei, the country's central intelligence agency.⁵ As early as 1961, the first high-ranking BND delegation traveled to Taiwan and agreed to comprehensive cooperation.⁶ In return, Taiwan maintained an intelligence mission in Pullach. This cooperation was never significantly impaired, despite the Federal Republic of Germany establishing diplomatic relations with the People's Republic of China and simultaneously severing ties with the *Republic of China on Taiwan (ROC)* on October 11, 1972. On the contrary, the BND office in Taipei saw its staff increased last year. And when representatives of Taiwanese intelligence services are in Germany, they are transported across the country in a private jet.⁷

Nevertheless, as society became more democratic, Taiwan's security services appeared to have long neglected—and perhaps even downplayed for political reasons—the threat posed by espionage and cognitive warfare in all its forms emanating from mainland China. For instance, Taiwanese agents are said to have been withdrawn from China during President Ma Ying-jeou's term in office (2008–2016).⁸

And the Ministry of Justice Investigation Bureau (MJIB, 法務部調查局), the Taiwanese counterpart to the American FBI, which is responsible for counterintelligence,

did not decide until January 2024 to address this pressing issue more intensively through a combined special unit. With the establishment of the Cognitive Warfare Research Center (法務部調查局認知戰研究中心, MJIB Cognitive Warfare Research Center), the agency decided to expand its structures by merging various departments tasked with these responsibilities into a powerful unit.⁹

This article was written as part of the Taiwan Fellowship program of the Taiwanese Ministry of Foreign Affairs. Although the topic was chosen by the author himself and, needless to say, there was not the slightest influence on the research findings from Taiwanese government agencies, the project is a sensitive one. This is because the present research project could not have succeeded without contacts and cooperation with security and intelligence agencies as well as representatives of foreign governments in Taiwan.

But intelligence agencies are, after all, not public services. Such “cooperation” requires trust. Interlocutors must not be named. Certain sources cannot be fully disclosed without harming informants or revealing classified information to their adversaries. In some chapters of this study, the author therefore deemed it appropriate and indeed necessary to depart from the citation practices customary in academia. Instead, the author has adopted the practice common in journalism of simply labeling certain informants and information as “background discussions.”

The aim of this work was to classify Taiwan's current threat situation not only in military terms but as a multidimensional network of psychological, legal, and strategic warfare. Particular attention, however, is to be paid here to China's espionage, primarily against Taiwan but also against the rest of the world.

Just how accute the infiltration of Taiwan by the PRC's security agencies really is is illustrated by a personal experience that befell the author of this study at the beginning of his research in Taiwan and serves as an excellent case study of Chinese infiltration.

In June 2025, one of Germany's most renowned journalists visited us, and we drove to Alishan, a well-known tourist destination in central Taiwan. There were four of us when a younger woman approached me and asked if I could take a photo of her. I was happy to oblige, but I soon noticed her strong northern Chinese accent. And as I was walking away, I asked her, "But you're not from Taiwan, are you?" Her answer: "No, I'm from China." That piqued my curiosity, because currently the government in Beijing no longer issues exit permits for its citizens to travel to Taiwan. So, I asked how that could be possible given the broader political climate. ^[9] She said, "I live in Denmark." As she immediately added, in the very north of the country. But that is where the strategically important waterway, the Skagerrak, is located, through which all shipping traffic from the Baltic Sea to the North Sea passes. I became suspicious and ended the conversation.

But now things really got interesting. The woman picked up the phone I'd just used to take her picture and spoke to someone on the other end in a northern Chinese dialect, loud enough for us to hear clearly. On the way back to our hotel, we noticed that she hadn't just followed us there—she'd also sat down in the lobby, unnervingly close to our guest and his wife. See above, the scene from Switzerland; I had a hunch whose orders the woman was following. I assumed that the supposed Chinese tourist at Alishan must also be an agent of the *Ministry of State Security (MSS)* of the People's Republic of China.

That is why, upon my return to Taipei, I contacted the relevant unit of the MJIB. And there, my fears were confirmed. Photos from street surveillance cameras, which I was allowed to view, showed unequivocally how the woman had followed us all the way into our hotel lobby. Records from the immigration authorities show that she had already left Taiwan the following day. The Taiwanese security service subsequently informed the BND resident at the German mission and the intelligence service in Denmark. Even the National Security Council (國家安全會議) discussed the case.¹⁰

The fact that the threat posed by Chinese agents in Taiwan is already part of everyday life will be substantiated below. To begin with, however, here is an overview of how leading scholars define the debate on cognitive warfare in all its facets and nuances and draw the distinction from classical espionage as well as united front work.

Chapter 2 – In the Eye of the Storm: The Academic Debate on Cognitive Warfare and Hybrid Threats

In the hybrid conflict situations with which the Republic of China is confronted by the People's Republic of China, terminology often becomes entangled in a diffuse field of tension. To achieve a clear analytical distinction, it is essential to define the nuances between cognitive warfare, united front work, and traditional intelligence operations.

In the Taiwanese security debate, two experts who combine academic excellence with operational experience in the security apparatus are coming into focus: **Professor Kerry Gershaneck**, a longtime Pentagon strategist whose expertise in strategic communication and countering subversive influences has also been explicitly recognized by **President Lai Ching-te** (賴清德), and **Professor Liu Wen-ping** (劉文斌). As the former head of the research department at the Ministry of Justice Investigation Bureau (MJIB)—an agency whose function lies somewhere between that of the American FBI and the German Federal Office for the Protection of the Constitution (Bundesamt für Verfassungsschutz, the federal domestic intelligence agency)—Liu is now considered the most cited expert on the anatomy of Chinese influence.

2.1. Cognitive Warfare: Beyond FIMI

The international community is still struggling to arrive at a universally accepted

definition of cognitive warfare. Prof. Liu Wen-ping 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 falls short and is at the same time too vague, as the term could criminalize legitimate economic or cultural information flows. He illustrates this using the example of Taiwanese oolong tea exports: By definition, an advertising campaign for tea manipulates information to influence consumer behavior (manipulation) and shift market shares (interference). According to strict FIMI logic, Taiwan would thus be waging cognitive warfare against Europe¹¹.

Building on classical persuasion models from communication research, Liu Wen-ping 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.”¹²

This approach clearly distinguishes cognitive warfare from legitimate soft power or advertising, as it focuses on the malicious political objective and the targeted behavioral change.

2.2. The United Front: Instrumentality Rather Than Friendship

A common misunderstanding in Taiwan is the reduction of United Front work to the mantra “win over secondary enemies to defeat the main enemy.” According to Liu Wen-ping, this view is incomplete, as the Chinese Communist Party (CCP, 中共) also “co-opts allies to defeat the main enemy.” The United Front, declared by **Mao Zedong** (毛澤東) to be one of the three “magic weapons” (法寶), is not a traditional intelligence service, but rather a political mobilization tool. **Liu defines it precisely: “The Communist Party forms**

friendships with people outside the party in order to mobilize these friends to support the party’s political goals.”¹³

The concept of “**instrumental** friendship” is key here. These “friends” are tools for achieving objectives. While classic espionage (Spy War) aims to steal secrets, the United Front aims to corrupt decision-making and create an internal layer of collaborators.

2.3. Hybrid Warfare and the Gray Zone

Hybrid warfare often defies a clear temporal distinction between peace and war. It combines conventional military threats with non-traditional means such as psychological warfare, economic coercion, and cyberattacks.

Table II-1 | Comparison between conventional and hybrid warfare

Characteristic	Conventional Warfare	Hybrid Warfare
Mode	Regular troops, invasion, overt violence.	A mix of military, psychology, crime, and diplomacy.
Time	Clear separation (declaration of war).	Permanent instability (no peace, no war).
Goal	Occupation of territory, overthrow of the government.	Capitulation of the enemy through internal collapse or coercion.
Example	Iraq War (2003).	Ukraine (since 2014), U.S.-Iran conflict.

Source: Author’s own illustration based on Chen Yu-sheng and Zhong Zhang-han (2022) as well as Liu Wen-ping (2025).

The **gray zone** describes the specific space below the threshold of open military conflict. The RAND Corporation identifies the “salami-slicing” tactic as a central element here: Small, hard-to-track provocations that individually do not justify military retaliation but, taken together, shift the status quo in Beijing’s favor¹⁴. Current examples include the cutting of undersea cables or the disabling of *Automatic Identification Systems* (AIS) on ships in the waters around Kinmen.¹⁵

2.4. The Interaction of Spheres

Prof. Liu Wen-ping’s contribution lies in the graphical representation of the relationship between these concepts (see *Table 1*). He posits that united front work and cognitive warfare are not isolated phenomena, but integral components of hybrid warfare that span all phases of a conflict.

- **Peace Phase:** This is where the groundwork is laid. **Soft power campaigns and the cultivation of “instrumental friends”** create networks that can be activated in an emergency.
- **Gray Zone Phase:** Cognitive warfare turns vicious. Narratives such as “anti-Americanism” (疑美論) or the defamation of the Taiwanese army’s

combat effectiveness are disseminated to undermine confidence in the country’s own defense capabilities¹⁶.

- **War Phase:** The cognitive component aims to **completely demoralize the civilian population and political leadership** in order to provoke poor decision-making.
- **Post-war Phase:** Here, **cognitive warfare transforms into a “cognitive civil war”** within the occupied territory to legitimize the new order and nip resistance in the bud.

2.5. Conclusion: Synergy of Destabilization

Kerry Gershaneck and Liu Wen-ping conclude that **Taiwan serves as a “laboratory” for this new form of conflict. The line between espionage (the theft of data) and the united front (the manipulation of people) is blurring.** While the “spy war” operates in the shadows, the united front operates in broad daylight within civil society. **Only through a clear conceptual distinction and an understanding of the mutual reinforcement of cognitive narratives and personal networks can Taiwan develop an effective defense strategy.**¹⁷

Chapter 3 – The Architecture of the “Secret Front.” The Genesis of Chinese Intelligence Services versus the KMT and Taiwan.

The history of Chinese intelligence services is inextricably linked to the paranoia and boundless ruthlessness of an underground organization. Unlike state services, which operate under a constitution, the CCP’s services have, since their inception, followed a revolutionary logic in which morality is subordinate to absolute party discipline.

3.1. The Era of the “Red Brigade”: Zhou Enlai and the Professionalization of Terror

The myth of the “clean diplomat” **Zhou Enlai** (周恩來) often obscures his role as the founder of a highly efficient terror apparatus and the communist secret service. After the split with the *National Kuomintang Party (KMT)* in 1927, he created the **Teke** (特科). The most notorious unit was the “Third Section,” known as the **Red Brigade** (紅隊).¹⁸

- **Systematic Massacres and “Elimination of Traitors”:** Under Zhou’s direct leadership, the Red Brigade operated as an execution squad. The best-known example of the brutality of those years is the 1931 case of **Gu Shunzhang** (顧順章). After Gu, himself a high-ranking intelligence officer, defected to the KMT, Zhou Enlai personally ordered the murder of Gu’s entire family. Over 30 people, including

women, children, and uninvolved relatives, were strangled in Shanghai and buried in the garden to avoid drawing attention with gunshots. **This uncompromising harshness was intended to ensure that loyalty within the “United Front” remained unchallenged**¹⁹.

- **The Subversion of the KMT:** The CCP’s infiltration of the Nationalists was not a side effect, but a complete takeover. Agents such as **Qian Zhuangfei** (錢壯飛) worked at the heart of the KMT’s intelligence service and forwarded every dispatch to Mao Zedong. **Weng Yanqing** (翁衍慶) former deputy director of Taiwan’s Military Intelligence Bureau (MIB), describes how the KMT often operated “blind and deaf” because its own staff was infiltrated by **CCP cadres**. These agents acted with a mixture of ideological fanaticism and cold calculation that permanently destroyed trust within the KMT²⁰.

3.2. The “Magic Weapon”: The United Front (統一戰線)

Mao Zedong described the **United Front**, alongside the Red Army and party building, as one of his three “magic weapons.” Its function remains essential to this day for understanding the strategy toward Taiwan.

- **Concept of Subversion:** The United Front is not a traditional intelligence service, but rather an apparatus for political warfare. Its task is to “isolate enemies and win over friends”—whereby “friends” are often “useful idiots” in the Leninist sense, who cooperate in the short term and must be neutralized in the long term. (Research sometimes refers to them as “unwitting collaborators”)
- **The Method:** It uses legal structures—business associations, academic institutions, and cultural organizations—to sow pro-Chinese narratives. In Taiwan, the united front aims to undermine social cohesion by stoking divisions and binding elites through economic incentives (bribery) or political promises. It is this “silent infiltration” that lays the groundwork for intelligence-driven blackmail.²¹

3.3. Intelligence Agencies in Mao Zedong’s Red People’s Republic

With the founding of the *People’s Republic of China (PRC)* in 1949, the systematic establishment of a state security apparatus began. In the early years under Mao Zedong, the primary focus was on securing political power. Institutions for political control and counterintelligence became central instruments of the new government.²²

The **Ministry of Public Security** (公安部), which was responsible for internal security and political surveillance, played an important role during this phase. However, the

institutional landscape of the intelligence services remained fragmented at first. Various agencies and party organizations performed functions that were, in part, similar in the area of intelligence gathering.²³

It was not until **1983** that a fundamental organizational restructuring took place. With the establishment of the **Ministry of State Security** (國家安全部), a central institution was created that brought together several previously separate structures. This ministry rapidly developed into the most important civilian intelligence service of the People’s Republic.²⁴

3.4. Institutional Structure and the “Xi Revolution”

Since Xi Jinping took office, this historically evolved apparatus has been radically centralized. The **National Security Commission** (中央國家安全委員會), established in 2014, now pulls all the strings:

- **Ministry of State Security (MSS)** (國家安全部): Focuses on global espionage and countering foreign influence. It applies historical lessons on infiltration to modern cyber operations.
- **Ministry of Public Security (MPS)** (公安部): Responsible for internal repression and the surveillance of the “five toxic groups” (including Taiwan independence advocates).
- **Strategic Support Force** (戰略支援部隊): The technological spearhead for cyber warfare against Taiwan’s infrastructure.

3.5. The New Legal Landscape: Espionage as a Civic Duty

Beijing has transformed decades of secrecy into a tightly woven legal system **capable of compelling every Chinese citizen worldwide to cooperate and engage in espionage**:

- **National Security Law (2015)**: It asserts sovereignty over Taiwan and **defines any form of resistance as a criminal act against the state**.
- **National Intelligence Service Law (2017)**: Articles 7 and 14 **oblige citizens and companies to actively assist in espionage**. For Taiwan, this means that any economic exchange is a potential vector for infiltration.
- **Counterespionage Law (2023)**: A tightening of the law that allows for the detention of any foreigner or Taiwanese citizen on “suspicion.” This practice is commonly described in research and the media as “hostage diplomacy.”²⁵

Table III-1 | Ministers of State Security since 1983.

*The MSS (Ministry of State Security, 國家安全部) was founded in 1983 and is the People’s Republic of China’s primary civilian foreign intelligence service.*²⁶

Name	Chinese	Term	Brief Biography & Focus
Ling Yun	凌雲	1983–1985	First Minister; established the basic structures of the security apparatus.
Jia Chunwang	賈春旺	1985–1998	Long-term consolidation; later Attorney General.
Xu Yongyue	許永躍	1998–2007	Focus on international operations and traditional counterintelligence.
Geng Hui-chang	耿惠昌	2007–2016	Massive expansion of the cyber and technology intelligence sectors.
Chen Wenqing	陳文清	2016–2022	Close ties to Xi Jinping; promotion to the Politburo of the CCP.
Chen Yixin	陳一新	since 2022	Current head; focus on geopolitics and national security.

3.6. Conclusion: The Continuity of Violence

A clear thread 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

rather as targets of far-reaching infiltration. The brutality of the early years has now given way to a technocratic, legally disguised form of oppression, which nevertheless pursues the same goal: the complete political paralysis of the opponent through the “Secret Front,” that is, its intelligence services.

Chapter 4 – The Power of Sheer Numbers. Personnel and Structures

4.1. Numbers Matter

The intelligence services of the People’s Republic of China follow an organizational logic that differs in key respects from the structure of Western intelligence systems. While many Western services are deliberately kept relatively compact

and rely heavily on highly specialized operations, the Chinese system takes a different approach. **It combines professional intelligence organizations with a wide-reaching network of state institutions, party structures, scientific institutions, and economic organizations.**

Figure 1 | Structure of the Chinese intelligence system



This combination results in an organizational breadth that is frequently described in international research as one of the defining characteristics of the Chinese intelligence system. **To put it another way: the CCP and the PRC, in their current form,**

cannot function or survive without engaging in massive espionage and constant surveillance of their own population, or without stealing the intellectual property of other countries and systems.²⁷

Table IV-1 | Structure of the Chinese Intelligence System

Name	Name in Chinese
The Communist Party of China	中國共產黨中央委員會
Ministry of State Security	國家安全部
Provincial MSS Offices	省國家安全廳 / 市國安局
People's Liberation Army	中國人民解放軍
Strategic Support Force	戰略支援部隊
United Front Work Department	統一戰線工作部
Social Networks (Business, Universities, Diaspora)	社會網絡 (企業、高校、僑民)

The true strength of this system lies less in individual spectacular operations and more in its structural logic. The Chinese leadership relies on the principle of sheer mass: **when enough actors gather information, establish contacts, or exert influence, a dense network of data, relationships, and opportunities emerges over time. From this perspective, intelligence is not merely the activity of specialized agencies, but part of a comprehensive political system.**²⁸

The expression “power of sheer numbers” therefore describes less a precisely measurable quantity than a strategic mindset.

While traditional 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.²⁹

This model is particularly effective in the context of Taiwan policy. The proximity between the two societies—economically, culturally, and historically—creates numerous points of contact. For Chinese intelligence services, these contacts open up opportunities to gather information, build networks, and exert influence in the long term.

Table IV-2 | The intelligence apparatus is based on three pillars with massive staffing³⁰

Institution	Chinese designation	Functional role	Staff strength (approx.)
MSS	中華人民共和國國家安全部	Civilian foreign intelligence	110,000 (Headquarters) – 800,000 across all provinces and abroad
MPS	中華人民共和國公安部	Domestic Intelligence Service/ Police	500,000 (headquarters) – 2 million
PLA	資訊支援部隊 (ISF)	Military Cyber/ SIGINT	200,000 – 250,000

Note: These figures are based on estimates by Taiwanese and international intelligence agencies. Since the personnel strength of Chinese intelligence agencies is considered a state secret, these figures can only be approximate. (Compiled from reports by the Ministry of Justice Investigation Bureau (MJIB), Taipei 2026.)

In comparison, other intelligence agencies appear:

Table IV-3 | Comparison Table of Major Intelligence Agencies³¹

Service	Country	Estimated Staff Size	Structure
MSS	China	Approx. 800,000	Civilian foreign intelligence
CIA	USA	approx. 20,000	Strategic foreign intelligence
FSB	Russia	approx. 200,000	Internal security
MI6	United Kingdom	approx. 3,500	Foreign intelligence
DGSE	France	approx. 7,000	Military intelligence
BND	Germany	approx. 6,500	Strategic foreign intelligence

4.2. At the Heart of the Surveillance Apparatus – The MSS

At the heart of China's intelligence architecture are several state institutions whose responsibilities partially overlap and complement one another. **The most important civilian intelligence organization is the Ministry of State Security (國家安全部).**

Its responsibilities range from traditional foreign intelligence and counterintelligence to domestic political security. Over the past decades, the scope of this organization's activities has expanded significantly. In addition to political and military intelligence, the collection of economic and technological data now plays a key role.

Table IV-4 | Structure of the Ministry of State Security (MSS)

中華人民共和國國家安全部

Bureau No.	Function (English)	Chinese designation	Focus
1st Bureau	Confidential Affairs Bureau	機要局	Confidential communications, cryptography and related management
2nd Bureau	International Intelligence Bureau	國際情報局	Collection of international strategic intelligence
3rd Bureau	Political and Economic Intelligence Bureau	政經情報局	Collection of foreign political, economic and technological intelligence
4th Bureau	Hong Kong, Macau, and Taiwan Intelligence Bureau	港澳台地區情報局	Intelligence operations concerning Hong Kong, Macau and Taiwan
5th Bureau	Intelligence Analysis and Reporting Bureau	情報分析通報局	Intelligence analysis, reporting and guidance for intelligence collection
6th Bureau	Operations Guidance Bureau	業務指導局	Guidance of provincial and municipal state security organs
7th Bureau	Counterespionage Bureau	反間諜情報局	Collection of counter-espionage intelligence
8th Bureau	Counterespionage Investigation Bureau	反間諜偵察局	Tracking, investigation and arrest of foreign spies
9th Bureau	Internal Security Investigation Bureau	對內保防偵察局	Counterespionage protection involving foreign-related organizations and monitoring of domestic organizations and foreign institutions

Bureau No.	Function (English)	Chinese designation	Focus
10th Bureau	Foreign Security Investigation Bureau	對外保防偵察局	Monitoring of personnel and students abroad and investigation of overseas activities
11th Bureau	Intelligence Data Center Bureau	情報資料中心局	Collection and management of documentary intelligence and information
12th Bureau	Social Investigation Bureau	社會調查局	Public-opinion and broader social investigations.
13th Bureau	Technical Investigation Bureau	技偵科技局	Management and development of technical-investigation equipment and technology
14th Bureau	Technical Investigation Bureau	技術偵察局	Inspection of mail and technical surveillance of telecommunications
15th Bureau	Comprehensive Intelligence Analysis Bureau	綜合情報分析局	Comprehensive intelligence analysis and assessment
16th Bureau	Imagery Intelligence Bureau	影像情報局	Political, economic and military imagery intelligence, including satellite imagery analysis
17th Bureau	Corporate Bureau	企業局	MSS-affiliated enterprises, companies and other institutions
18th Bureau*	Counterterrorism Bureau	反恐局	Counterterrorism

**Note: Bureau 18 (Counterterrorism Bureau / 反恐局) is reported in recent open-source listings, but its numbering and organizational status are not consistently documented. Earlier sources identified a Counterterrorism Bureau as the “18th Bureau,” while more recent research has reported the 18th Bureau as responsible for U.S. operations and the Counterterrorism Bureau as the 19th Bureau. The exact current internal structure of the MSS therefore remains difficult to verify from open sources.*

Each Chinese province also has its own Provincial Department of State Security (省國家安全廳). These regional offices work closely with local Party structures, universities, and businesses. Formally, they report to the central leadership in Bei-

jing, but they enjoy considerable operational autonomy. **This structure plays a particularly important role in the context of Taiwan policy. Provinces along the Taiwan Strait—especially Fujian (福建省)—serve as key hubs for economic and social ties.**

4.3. The Ministry of Public Security (MPS)

With approximately 2 million regular police officers, the Ministry of Public Security (MPS) (中華人民共和國公安部) constitutes China's largest executive apparatus in terms of personnel. While its core mission lies in traditional policing, a significant portion of the apparatus—estimated at between 300,000 and 500,000 officers—functions as a **de facto domestic intelligence service**. This branch is concentrated in particular within the “Political Security” Department (First Bureau), which is tasked with safeguarding the Communist Party's rule against any form of internal opposition.

In operational espionage, the MPS plays a central role in the surveillance and **repression of dissidents as well as religious and ethnic minorities**. In doing so, the service utilizes a dense network of physical presence and state-of-the-art technological surveillance. **These activities are not limited to Chinese territory; as part of its operations, the agency targets individuals worldwide to exert political influence or pressure exiles to return.**

Another focus of the MPS is **comprehensive cyber surveillance and control of the digital space**. Through the administration of the “Great Firewall” and the monitoring of social media, the MPS generates enormous amounts of data that not only serve domestic stability but are also used to identify and infiltrate networks abroad. Thus, the MPS forms the backbone of

comprehensive social control, which is legally cemented by the National Intelligence Law.³²

4.4. Military Intelligence Services and Information Warfare

In addition to civilian intelligence services, military structures also play a central role in China's information system. **As part of the military reforms since 2015, the Strategic Support Force (戰略支援部隊) was established within the People's Liberation Army. This organization consolidates capabilities in several strategic areas: cyber operations, electronic reconnaissance, satellite reconnaissance, and information warfare.**³³

4.5. Social Networks as Multipliers

One of the most notable features of the Chinese system lies outside the realm of traditional intelligence services. Organizations such as the United Front Work Department (統一戰線工作部) coordinate political and social networks, some of which are also used for information gathering. These networks include, among others, scientific collaborations, economic organizations, diaspora networks, and cultural exchange programs. In research, this model is often described as a “whole-of-society approach.”

4.6. Taiwan as a Key Target of Chinese Intelligence Activities

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. **Accordingly, the collection of political, military, and social intelligence on Taiwan plays a central role.** Today, China's information strategy toward Taiwan encompasses several interconnected dimensions: military intelligence, political influence operations, and econom-

ic intelligence gathering. The province of Fujian (福建省) serves as a geographically proximate operational hub in this regard.³⁴

According to information from the author of this study, approximately 180,000 agents from the PRC's security apparatus work exclusively on the "issue" of Taiwan.³⁵

Table IV-5 | Programs to Promote Integration Between Mainland China and Taiwan³⁶

Unit	Function / Program Name	Chinese Name
Fujian Province	West Coast Economic Zone	海峽西岸經濟區
Pingtán	Pingtán Comprehensive Pilot Zone	平潭綜合實驗區
Xiamen–Kinmen	Integrated Development Demonstration Zone	金廈兩岸融合示範區
Various Provinces	Startup Parks for Taiwanese Youth	臺灣青年創業園區
Various cities	Houses of Taiwanese Compatriots	青之家

Officially, these programs pursue economic goals, but they create institutional networks through which contacts with political and economic elites in Taiwan can be established.

Chapter 5 – Shadows on the Net. The Role of 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, known in the field as **Advanced Persistent Threats (APTs)**, play a significant role in this. **These units do not operate in a vacuum; they are firmly embedded in the power structure of the People's Republic** and are subordinate either to the MSS or to the newly formed **Information Support Force (ISF – 信息支援部隊)** of the People's Liberation Army (PLA)³⁷.

Analysis of the years 2024–2025 reveals a specialization that goes far beyond mere data theft. It involves the “preparation of the digital battlefield” (戰場準備).

5.1. Volt Typhoon: Sabotage of Critical Infrastructure (MSS/PLA – Hybrid)

This group, which often operates under cover names in China, is currently considered the most dangerous threat to **critical infrastructure (KRITIS – 關鍵基礎設施)**. Its focus is less on espionage and more on potential sabotage.

- **Goal:** Systematic infiltration of **water utilities, power grids, and transportation systems in the U.S., Guam, and Taiwan.**

- **Tactics: “Living off the Land” (LotL).** Instead of injecting conspicuous malware, they use legitimate system tools already present on the target computers. In China, this inconspicuous method of infiltration is often understood as part of “**shadow warfare**” (影子戰爭).
- **Strategic Purpose:** In the event of a **conflict in Taiwan, these “sleeper accounts” are to be activated** to paralyze Allied logistics and instill **panic among the civilian population** through targeted blackouts³⁸.

5.2. APT41 (Affiliated with: MSS – Office 10/11 in Chengdu/Sichuan)

APT41 (雙龍) is a highly professional unit that pursues a **dual strategy of state espionage and financially motivated cyber-crime.**

According to experts, it is believed to be a state-sponsored Chinese hacking group that operates under various names. Its Chinese name is **Double Dragon (雙龍)**. They are also tracked under various other monikers by different security vendors, including **Winnti, Barium, Axiom, Wicked Panda** (by CrowdStrike), and **Bronze Atlas** (by Secureworks). APT41 is notable for conducting both espionage operations on behalf of the Chinese government and **financially**

motivated cybercrime — a dual mandate that makes them relatively unique among nation-state threat actors. In August 2019 and September 2020, the U.S. Department of Justice filed charges against **five Chinese and two Malaysian nationals**, all of whom were linked to a company named **Chengdu 404 Network Technology Co., Ltd.** This company is believed to be a front for APT41 activities.³⁹

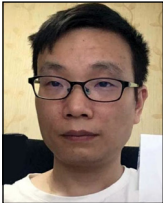
- **Objective:** Massive **theft of intellectual property (IP)**, particularly in the fields of **semiconductor technology** (半導體) and biotechnology.
- **Tactics:** **Supply chain attacks** (供應鏈攻擊). The group infiltrates software manufacturers to **distribute malicious code via official updates to thousands of end users worldwide—a digital “Trojan horse” in the global supply chain**⁴⁰.

Figure 2 | Members of the APT-41 group who are wanted by the FBI.

**WANTED
BY THE FBI**

APT 41 GROUP


ZHANG Haoran TAN Dailin QIAN Chuan


FU Qiang JIANG Lizhi

CAUTION

ZHANG Haoran, TAN Dailin, QIAN Chuan, FU Qiang, and JIANG Lizhi are all part of a Chinese hacking group known as APT 41 and BARIUM.

On August 15, 2019, a Grand Jury in the District of Columbia returned an indictment against Chinese nationals ZHANG Haoran and TAN Dailin on charges including Unauthorized Access to Protected Computers, Aggravated Identity Theft, Money Laundering, and Wire Fraud. These charges primarily stemmed from alleged activity targeting high technology and video gaming companies, and a United Kingdom citizen.

On August 11, 2020, a Grand Jury in the District of Columbia returned an indictment against Chinese nationals QIAN Chuan, FU Qiang, and JIANG Lizhi on charges including Racketeering, Money Laundering, Fraud, Identity Theft, and Access Device Fraud. These charges stem from their alleged unauthorized computer intrusions while employed by Chengdu 404 Network Technology Company. The defendants allegedly conducted supply chain attacks to gain unauthorized access to networks throughout the world, targeting hundreds of companies representing a broad array of industries to include: social media, telecommunications, government, defense, education, and manufacturing. These victims included companies in Australia, Brazil, Germany, India, Japan and Sweden. The defendants allegedly targeted telecommunications providers in the United States, Australia, China (Tibet), Chile, India, Indonesia, Malaysia, Pakistan, Singapore, South Korea, Taiwan, and Thailand. The defendants allegedly deployed ransomware attacks and demanded payments from victims.

If you have any information concerning these individuals, please contact your local FBI office, or the nearest American Embassy or Consulate.

Field Office: Washington D.C.

www.fbi.gov

Source: Federal Bureau of Investigation.
“Wanted by the FBI: APT 41 Group.” U.S.
Department of Justice, September 3, 2020.
Retrieved March 25, 2026, from: [https://
www.justice.gov/opa/press-release/
file/1317056/download](https://www.justice.gov/opa/press-release/file/1317056/download)

5.3. RedAlpha / RedJuliett (Affiliated with: MSS – Bureau 4 in Fuzhou/Fujian)

Due to their geographical proximity to the Taiwan Strait, these groups focus almost exclusively on the diplomatic and political sphere in Taipei. Their activities are closely linked to “united front work” (統一戰線).

- **Target:** Government agencies, **pro-democracy thinktanks, and religious organizations in Taiwan.**
- **Tactics:** Massive phishing and the creation of deceptively authentic clones of official Taiwanese government login pages **to steal login credentials from key individuals.** This form of “cognitive warfare” (認知戰) aims to compromise internal communication channels and spread disinformation⁴¹.

Table V-1 | Cyber Actors 2025/26

Group	Classification	Core Competence	Main Target Area
Volt Typhoon	PLA / MSS (Hybrid)	Infrastructure sabotage	USA, Guam, Taiwan
APT41	MSS (Bureau 10/11)	Industrial espionage	Global (Focus on Tech)
RedJuliett	MSS (Bureau 4 - Fujian)	Political Intelligence	Taiwan (Government)

Chapter 6 – The Facets of the CCP’s Cognitive Warfare in Democratic Countries, Including Taiwan.

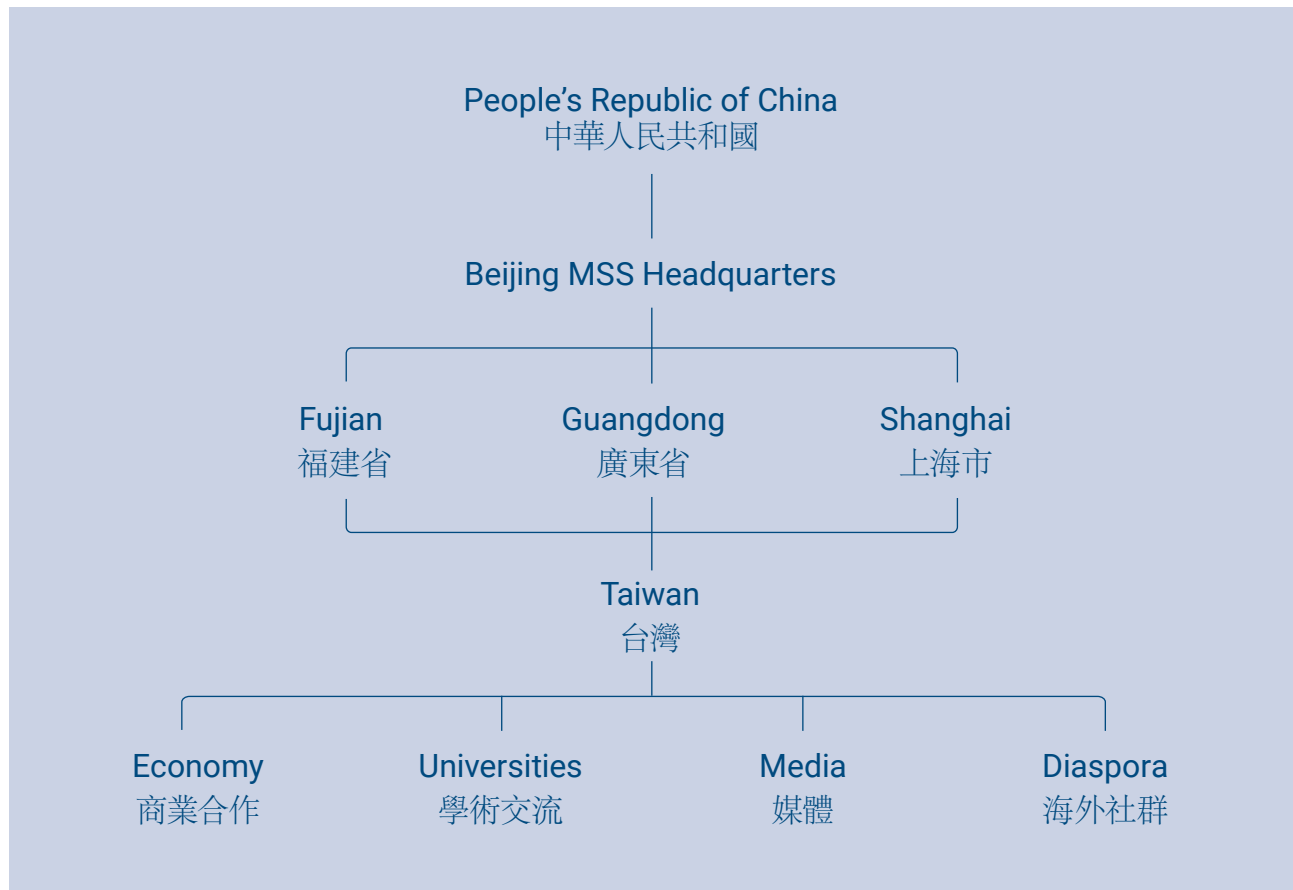
6.1. Background

The information in Chapter 6 is derived from extensive interviews with security services and affiliated analysts from think tanks in Taiwan (both local and international), as well as diplomats and military personnel. These therefore fall into the category known in journalism as “off-the-record interviews” (here: “Author interview confidential, 2025”). Specifically, this means that the sources cannot be named.

However, the author has verified the relevant facts using secondary sources. (See also: 展望與探索雜誌社. The Prospect & Exploration Magazine Society. Taipei, Taiwan, May 2025.) Additional sources are cited separately.)⁴²

It should also be noted that the terminology regarding Chinese military reforms and intelligence organization is in a state of flux. In this work, the terms are used according to their chronological context.

Figure 3 | Chinese Intelligence and Influence Networks Targeting Taiwan



In research, these regions are considered **important platforms for political influence and information gathering in the context of Taiwan policy.**

The CCP's influence operations are not isolated tactics, but systematic actions that serve the overall national strategy. Their fundamental driving force lies in maintaining the CCP's position of power and the socialist system, enhancing comprehensive national strength, ensuring territorial integrity and maritime rights, and the ultimate realization of the "Chinese Dream" (中國夢) of the "great rejuvenation of the Chinese nation" (中華民族偉大復興), as the party's two central slogans state.

This strategy is embedded within the framework of the "Comprehensive National Security Outlook" (總體國家安全觀), **which emphasizes placing national security at the forefront of all tasks** and viewing development and security as a mutually reinforcing relationship.

In concrete practice, the People's Liberation Army (PLA) has long placed emphasis on the application of **the "Three Wars" (三戰)**, namely "warfare through public opinion" (輿論戰), **"psychological warfare" (心理戰)**, and **"legal warfare" (法律戰).**

Warfare through public opinion aims to control the discourse, strengthen unity of thought internally, and **actively disseminate the "Chinese perspective" (中國觀點) and the "Chinese narrative" (中國敘事) externally, in order to counter ideological infiltration from the U.S. and Europe**

and eliminate the influence of the "China Threat Theory" (中國威脅論).

Psychological warfare focuses on **undermining the enemy's will and spreading mistrust and fear.** Legal warfare uses national and international law as a tool to cloak its own actions in a veneer of legitimacy and to weaken the defensive capabilities of other countries.

Currently, the CCP's influence operations against democratic countries have gone beyond the scope of traditional diplomacy and evolved into a multidimensional non-military strategy.

This includes **"information and cognitive warfare" (資訊與認知戰)**, **"economic coercion" (經濟脅迫)**, and **"political and social infiltration" (政治社會滲透).** Information warfare employs disinformation, large-scale foreign propaganda, and cyber espionage with **the aim of creating a "constructed reality" (被製造的現實),** manipulating public opinion, and undermining the public's perception of facts. Economic means leverage the vast market and supply chains to exert pressure on other countries, though studies show that their long-term impact is limited and may trigger counter-measures from the affected countries.

Political and social infiltration exploits the openness of democratic systems (民主體制的開放性) to destabilize and manipulate opponents from within through means such as "united front" organizations (統戰組織), overseas Chinese (海外僑民), students abroad (留學生), and political donations (政治獻金).

It should also be noted, however, that the United Front is not a homogeneous system, but rather comprises a multitude of organizations and networks with different functions and scopes of action. With technological development, however, these traditional methods of warfare have evolved into a more comprehensive concept of **“cognitive warfare”** (認知域作戰).

This strategic shift explains why China views the manipulation of influence (影響力操作) as a “struggle for security and supremacy” (安全和優勢之爭) in the realm of ideology against the U.S. and Europe, and not merely as propaganda (宣傳) in the traditional sense. This involves spreading lies and distorting facts. Through a state-level initiative (國家級行動), digital technology (數位技術), big data analysis (大數據分析), and psychological profiling (心理剖析) are used **to organizedly and systematically “create reality”** (製造現實).

The following is a brief explanation of the methods of information and cognitive warfare (資訊與認知戰), economic coercion (經濟脅迫), and political-social infiltration (政治社會滲透).

6.2. Methods of Information and Cognitive Warfare (資訊與認知戰)

Information and cognitive warfare (資訊與認知戰) is one of the core tactics of the CCP’s (中共) influence operations (影響力操作). The goal is to manipulate the infor-

mation environment (資訊環境), influence public opinion (公眾輿論), and ultimately undermine public confidence in the democratic system (民主制度) and the rule of law (法治).

a) Disinformation Tactics (虛假訊息戰術)

The channels through which **the CCP disseminates false information** (中共虛假訊息) **often follow an “inside-out”** (由內而外) **pattern**. For example, the information wars during the “Kansai Airport Incident” (關西機場事件) in 2018 and during the COVID-19 pandemic could be traced back to social media within China (such as Weibo (微博)). (Kansai: see note at the end of the chapter)

These were subsequently picked up by content farms (內容農場), cited by pro-Chinese media abroad (海外親中媒體) and local collaborators (在地協力者), and eventually penetrated mainstream social media (主流社群媒體) and forums in the target countries. **Disinformation often exploits social divisions** (社會分歧) **to sow chaos and unrest**, such as using the topic of “Indian migrant workers” (印度移工) to stir up conflict and panic within Taiwanese society.

Furthermore, official government documents (政府公文) or news reports (新聞報導) are forged to spread unconfirmed rumors (謠言) such as “city lockdowns” (封城) or “mass infections in hospitals” (醫院群聚感染).

b) Large-scale Overseas Propaganda and Media Infiltration (大外宣與媒體滲透)

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

This operational model also includes cooperation with local media to provide content (在地媒體進行內), the joint production of programs, and the use of commercial interests to exert pressure on media outlets and individuals. For example, journalists are offered trips to China, or internet celebrities (Key Opinion Leader, KOLs) are financially supported in creating content, while market access and advertising revenue are used to force companies and celebrities into self-censorship (自我審查).

Figure 4 | Example of a trip organized for Cambodian journalists to China in 2025



Source: The author’s diplomatic contact in Cambodia

c) Network Tools and Technologies

(網路工具與技術)

Leaked documents from the Chinese cybersecurity firm “I-Soon” (安洵) provided direct evidence of the CCP’s internet interventions. **The documents show that the company developed a special “Twitter and public opinion control system” (Twitter 與輿情導控系統) to manipulate public opinion abroad and suppress dissenting views.**

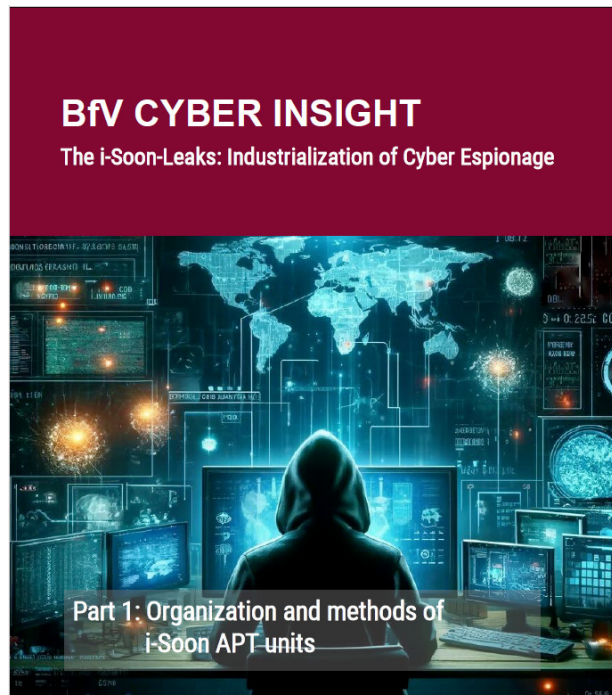
Chinese hacking groups also conduct cyberespionage against foreign governments and companies with the aim of stealing sensitive information and strategic insights—such as U.S. trade negotiation strategies or recordings of presidential phone calls—**targeting over 80 countries worldwide.** Methods such as “fake account network phishing” (假帳號網路釣魚) and “AI-generated news” (AI 生成新聞) make the sources of disinformation even harder to trace and complicate the defense efforts of democratic states.

d) Economic Coercion (經濟脅迫)

The CCP (中國共產黨) uses its enormous **economic clout as a strategic tool to exert economic coercion against countries that cross its “political red lines” (政治紅線).**

For example, in 2021, Lithuania’s approval of the establishment of a Taiwanese representative office drew the CCP’s ire, prompting it to immediately sever trade ties and exert pressure on multinational companies operating facilities in Lithuania.

Figure 5 | BfV Cyber Insight



Source: Federal Office for the Protection of the Constitution. August 1, 2024

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. Although the CCP’s coercive measures have short-term economic impacts, the long-term effect of such large-scale blackmail is relatively limited. The countries under pressure are actively tapping into new markets, and the CCP itself is ultimately forced to lift sanctions due to domestic demand.

This “backfire effect” (反噬效應) demonstrates that the CCP’s economic weapon is not invincible and that its effectiveness is constrained by the needs of its own domestic economy.

In sharp contrast to its actions of economic coercion, the CCP's official narrative portrays its economic strength as a contribution to globalization. This narrative emphasizes the strength and resilience of the CCP's economy and attributes this to the systemic advantage of "concentrating forces to accomplish major tasks" (集中力量辦大事).

The CCP has positioned itself as the "engine of global economic growth" (全球經濟增長的發動機) and as the "ballast stone for stabilizing global inflation" (穩定全球通脹的壓艙石). This narrative seeks to portray its stability and contribution to the global economy rather than viewing it as a geopolitical weapon. The dual nature of this economic narrative aims to obscure the true intentions of its economic strategy.

6.3. The Actors of Political and Social Infiltration (政治與社會滲透)

The political and social infiltration tactics of the CCP aim **to exploit the openness of democratic systems** (民主體制本身) **to destabilize opponents from within.**

a) United Front Work (統戰工作)

The goal of the operations conducted abroad by the United Front Work Department of the CCP Central Committee (中共中央統戰部) is **to influence overseas Chinese communities, foreign governments, and other actors to support a "Beijing-first" (北京優先) policy.**

For example, the United Front recruits community leaders in Taiwan, mobilizes "paid demonstrators" (走路工) for political protests, and uses "overseas police stations" (海外警僑驛站) to monitor dissidents, gather information, and intimidate overseas Chinese. These actions constitute "transnational repression" (跨國鎮壓) against overseas Chinese communities.

b) Students and Scholars (學生與學者)

The "Chinese Students and Scholars Association" (CSSA, 中國學生學者聯合會) **acts as overseas cells of the CCP at foreign universities.** They not only receive funding and instructions from the consulates but are also responsible for monitoring their fellow students and suppressing criticism of China. Such organizations are not only propaganda tools of the CCP but also serve the **function of "information gathering"** (信息採集) **and act as sleeper cells against their host countries.**

c) Lobbying and Political Donations (遊說與政治獻金)

The **CCP uses political donations and lobbying systems in democratic countries to infiltrate them.** In Australia, wealthy businesspeople of Chinese descent reportedly offered donations to major political parties to influence China-friendly policies. Similarly, Chinese technology companies such as Huawei and TikTok engage in large-scale lobbying in Europe to secure contracts for 5G expansion or improve their corporate image, which once again blurs the lines between business interests and national strategy.

d) Information Theft and Infiltration

(情報竊取與滲透)

Infiltration also includes covert activities aimed at stealing information. **For example, Chinese students and researchers in the U.S. steal trade secrets related to key technologies** such as chips and artificial intelligence (人工智能).

Chinese intelligence agencies also attempt to infiltrate the militaries of other countries, using funds or travel invitations to recruit retired or active-duty military personnel and **even urging them to “remain passive”** (消極不作為) **in the event of military actions by the People’s Liberation Army** (共軍) **against Taiwan.**

6.4. The Challenges for Taiwan

(對臺灣的挑戰)

Taiwan is widely **regarded as the “primary target”** (主要目標) **and “frontline laboratory”** (前線實驗室) **for the CCP’s influence operations** (影響力操作). The threats facing Taiwan include the combined use of information warfare (資訊戰), united front attacks (統戰), and political infiltration (政治滲透).

With regard to information warfare, frequent manipulation through disinformation campaigns can be observed in connection with the presidential election in Taiwan, the COVID-19 pandemic, and the incident involving the capsized fishing boat from Kinmen.

This information aims to divide Taiwanese society, sow distrust between the government and the public, and undermine public confidence in the democratic system.

The CCP also uses organizations such as its United Front Work Department (統戰部) and the Taiwan Affairs Office (國臺辦) to spread the narrative “both sides of the strait share the same origin” (兩岸同源) to Taiwanese youth, thereby increasing goodwill toward the CCP.

In the realm of media infiltration, the CCP’s official side disguises its political propaganda within seemingly independent reports through the illegal placement of marketing content (product placement) and joint content production to influence the Taiwanese media ecosystem and public opinion.

Nevertheless, public opinion polls indicate that the CCP’s united front, propaganda, and intimidation have not led to support for Beijing’s “One Country, Two Systems” (一國兩制) policy or a unification plan in Taiwan.

An opinion poll (民調) from April 2025 shows:

- 84.4% reject the “One Country, Two Systems” model.
- About **82.5% reject the claim that “Taiwan belongs to China and has never been a state.”**

- The Election Research Center at Chengchi University (政大選研中心) shows that the proportion of those who identify themselves as “Taiwanese” (自我認同為臺灣人) remains high, and support for maintaining the status quo or a tendency toward independence is far higher than the demand for unification.

Source: Mainland Affairs Council, April 24, 2025.
Retrieved December 31, 2025: www.mac.gov.tw

This illustrates that the majority of the Taiwanese population continues to view the CCP as “unfriendly/hostile” (不友善 / 具敵意) and opposes both military pressure and gray-zone pressure (灰色地帶施壓).

Overall, the CCP’s information and united front operations against Taiwan **are characterized by “agility and breadth”** (敏捷與廣泛); **they can quickly shape narratives in response to unpredictable events and apply long-term leverage in the economy and content industry.**

However, thanks to high vigilance in Taiwan and a mature fact-checking ecosystem (查核生態), short-term effects aimed at “influencing votes” (改票) are limited and have so far failed to undermine the fundamental identity or erode trust in the system.

Future risks include: the reduction in the cost of counterfeiting through AI synthesis technology, the expansion of self-censorship (自我審查) due to economic dependence, and local collaborators (在地協力者) who establish a “seamless connection” (無縫貼合) to local concerns.

6.5. In Background Discussions, Taiwan’s Security Agencies Have Summarized the Following Demands based on This Analysis

Transforming the network of local agencies (在地代理網路): At the political level, the following should be continued:

1. Strengthening transparent labeling and disclosure of financial flows (強化透明標示與金流揭露), follow the money,
2. Investment in local media and civic education (投資地方媒體與公民教育),
3. Developing guidelines for the disclosure of “conflicts of interest” (利益衝突) for key industries and internet celebrities (KOLs), as well as ...
4. ... rapid interagency responses and co-operation with international platforms to strengthen social resilience (以鞏固社會韌性).

6.6. The Security Organs of the CCP, Assessment and Classification regarding Threats to Regional, Asian, and International Security. Classification of Leaders

If we take the areas of “Party, United Front, Security” (黨、統戰、安全) as the basis for classification regarding institutions responsible for regional security issues, the most important body within the **Party** is the **Central Commission for National Security of the CCP** (中共中央國家安全委員會). In the **United Front** sector, **these** are

the Chinese People's Political Consultative Conference (全國政協) and the United Front Work Department of the CCP Central Committee (中共中央統一戰線工作部) within the security apparatus. With regard to the military, the Ministry of State Security (國家安全部) is the most significant.

a) Central Commission for National Security of the CCP (中共中央國家安全委員會).

In the communiqué of the Third Plenary Session of the 18th Central Committee of the CCP in November 2013, Xi Jinping proposed “establishing a National Security Commission, improving the national security system and national security strategy, and ensuring national security” (設立國家安全委員會, 完善國家安全體制和國家安全戰略, 確保國家安全).

Meng Jianzhu (孟建柱), then Secretary of the Central Committee's Political and Legal Affairs Committee, was entrusted with its **establishment**. In 2014, the CCP Central Commission for National Security (中共中央國安委) and its office were established. It no longer shares offices with the Central Leading Group for Foreign Affairs (中央外事工作領導小組) and was transformed into a commission specifically responsible for national security.

The General Secretary of the CCP Central Committee serves as chairman, while the Premier of the State Council and the Chairman of the Standing Committee of the National People's Congress serve as vice-chairmen. In May 2023, another vice-chairman was added, a position held

by **Cai Qi** (蔡奇), a member of the Politburo Standing Committee; he is also regarded as the person who is effectively responsible for national security affairs.

b) Chinese People's Political Consultative Conference (全國政協) and United Front Work Department of the Central Committee (中央統戰部)

The CCP's united front work (統戰工作) has long been led by a member of the Politburo Standing Committee who holds the chairmanship of the Chinese People's Political Consultative Conference (全國政協主席) (currently **Wang Huning** (王滬寧)).

Vice Chairman **Shi Taifeng** (石泰峰) was transferred in April 2025 from his position as head of the United Front Work Department of the Central Committee to head of the Organization Department of the Central Committee (中央組織部部長). **Li Ganjie** (李幹傑) (formerly Head of the Organization Department of the Central Committee) became the new Head of the United Front Work Department of the Central Committee.

The original purpose of establishing the Chinese People's Political Consultative Conference (CPPCC) was to win over figures from various parties and groups outside the CCP within the country. It embodies a strong sense of the United Front (統戰); therefore, the decision-making level of the CCP's United Front work (中共統戰工作) is led by a member of the Politburo Standing Committee who chairs the CPPCC, while practical implementation at the

operational level is carried out by the United Front Work Department of the Central Committee (中央統戰部).

On issues of regional security, the United Front departments (統戰部門) disseminate narratives that align with China's interests through official media or pro-China associations abroad, trade organizations, academic institutions, or social media. This serves to influence public opinion, weaken opposing narratives, infiltrate and win over individuals in other countries, and undermine opposition forces in other countries.

c) Ministry of State Security (國家安全部)

The Ministry of State Security (國家安全部) is **China's primary foreign intelligence**

and counterintelligence agency. Its main tasks include collecting and analyzing foreign intelligence, conducting counterintelligence missions, ensuring political security, and safeguarding national security. **The Ministry of State Security maintains branches throughout China and is considered China's largest and most active intelligence agency.**

In matters of regional security, the MSS works to shape a regional environment favorable to China by gathering intelligence on other countries, conducting counterintelligence operations, launching cyberattacks or manipulating information against other countries, and cooperating with the United Front Work Departments (統戰部門) on foreign infiltration.

Figure 6 | Overview of the structure of the Ministry of State Security of the PRC



Internal Departments

General Office	Counterespionage Bureau (Bureau 7)	Technical Investigation Bureau (Bureau 14)	Comprehensive Planning Bureau
Confidential Affairs Bureau (Bureau I)	Counterespionage Investigation Bureau (Bureau 8)	Comprehensive Intelligence Analysis Bureau (Bureau 15)	Administrative Management Bureau
International Intelligence Bureau (Bureau II)	Internal Security Investigation Bureau (Bureau 9)	Imagery Intelligence Bureau (Bureau 16)	Bureau of Retired Cadres
Political and Economic Intelligence Bureau (Bureau III)	Foreign Security Investigation Bureau (Bureau 10)	Corporate Bureau (Bureau 17)	Archives Office
Hong Kong, Macau, and Taiwan Intelligence Bureau (Fourth Bureau)	Intelligence Data Center Bureau (Bureau 11)	Political Department (Vice-Ministerial Level)	
Intelligence Analysis and Reporting Bureau (Bureau 5)	Social Investigation Bureau (Bureau 12)	Legal Awareness Office	
Operations Guidance Bureau (Bureau 6)	Technical Investigation Bureau (Bureau 13)	Education and Training Department	

Directly Affiliated Institutions

- China Institute of Contemporary International Relations
- School of International Relations
- Zhejiang Second People's Police University (Hangzhou Campus of the School of International Relations)
- Jiangnan Social Sciences Institute (Administrative College of the Ministry of State Security)

Vertically Managed Units



Beijing
Municipal
State Security
Bureau

Shanghai State
Security Bureau

Tianjin Municipal
State Security
Bureau

Chongqing Municipal State
Security Bureau

Liaoning Provincial State Security
Department

Shaanxi Provincial State Security
Department

Heilongjiang Provincial State Security
Department

Hebei Provincial National Security
Department

Shanxi Provincial State Security
Department

Jilin Provincial State Security
Department

Henan Provincial National Security
Department

Hubei Provincial State Security
Department

Hunan Provincial State Security
Department

Jiangxi Provincial Department of
State Security

Anhui Provincial Department of
State Security

Guangdong Provincial National
Security Department

Fujian Provincial State Security
Department

Zhejiang Provincial State Security
Department

Jiangsu Provincial State Security
Department



**People's Liberation
Army of China**

@ Strategic Support Force Network Systems Department (Unit Number: 32069)

**@ Former General Staff Department Technical Reconnaissance Department (Third Department)
Former General Staff Department Electronic Warfare Department (Fourth Department)**

**@ Central Military Commission Strategic Planning Office Network Information Coordination
Bureau**

**@ Joint Staff Department Intelligence Bureau, Central Military Commission (Formerly Second
Department of the General Staff Headquarters)**

**@ Liaison Bureau, Political Work Department, Central Military Commission (formerly Liaison
Department, General Political Department)**

@ Ministry of Public Security Political Security Bureau (Bureau 1)

Source: Training materials from an intelligence agency of the Republic of China (ROC) in Taiwan.
(See also Chapter 5, List of individual MSS offices.)

6.7. What are the Main Targets of the Chinese Security Agencies ...

a) ... with regard to Taiwan?

The CCP pays close attention to many aspects of Taiwanese society, such as:

- the areas of cross-strait relations (兩岸關係)
- the military in academic research
- the semiconductor sector in industry
- various segments of society

At this stage, the primary focus of research and R&D capabilities is on the semiconductor sector (半導體).

In 2014, the State Council of China (中國國務院) published the “Guidelines for Promoting the Development of the National Integrated Circuit Industry” (《國家集成電路產業發展推進綱要》) and supports the development of the semiconductor industry as part of a comprehensive national strategy. In addition, the “Big Fund” (大基金) was established through fundraising to recruit talent from abroad on a large scale.

Since salaries in Taiwan’s semiconductor industry at that time could not yet compete with those in Japan or South Korea, this accelerated the exodus of Taiwanese semiconductor talent to China. According to statistics, from 2014 to the end of 2019,

a total of about three thousand Taiwanese semiconductor professionals went to mainland China, accounting for 7% of the total workforce in Taiwan’s semiconductor industry. In the early stages, the talent moving to China consisted primarily of high-level executives, but this gradually shifted to a large number of mid-level engineers.

These engineers came predominantly from second-tier semiconductor manufacturers. At top-tier manufacturers such as TSMC (台積電), the proportion of talent leaving was relatively low due to salary and benefits as well as technological advantages. During this period, the CCP attracted Taiwanese semiconductor talent mainly through material incentives, positions of power, and future prospects.

After 2019, however, the trend of Taiwanese semiconductor talent migrating to China gradually slowed and even showed signs of a reversal.

This was due to the trade sanctions against China initiated by the U.S., technology embargoes, and the subsequent invitation to TSMC to establish factories in the U.S. The reasons for this are believed to be that compensation and prospects for employees in Taiwan’s semiconductor sector are viewed optimistically, the complete industrial chain—led by TSMC—has taken a leading global position, and geopolitical risks in cross-strait relations (兩岸關係) have steadily increased, dampening talent’s willingness to go to China.

As the direct poaching of talent became more difficult for the CCP, it shifted to acquiring Taiwanese semiconductor technology through other means. This includes:

- The acquisition of or investment in Taiwanese companies through covert capital operations
- Establishing technical partnerships with Taiwanese manufacturers investing in China
- Offering scholarships or internship opportunities to students in semiconductor-related fields
- Obtaining relevant parameters through upstream and downstream supply chains collaborating with Taiwanese manufacturers
- The acquisition of technology through covert illegal means such as industrial espionage and cyberattacks in third countries (涉外影響力)

b) Organs and working methods. The “central kitchen” principle (中央廚房). Which functional units and levels within the CCP apparatus are responsible for coordinating “influence abroad” (涉外影響)?

The CCP models its organizational structure on that of the Soviet Union. Since the party’s founding, the Organization Department (組織部) and the Propaganda

Department (宣傳部) have been established internally (the United Front Work Department (統戰部) and the Department of International Liaison (對外聯絡部) were added later). Mao Zedong once said: **“The revolution rests on these two pillars: the pen (筆桿子) and the gun (槍桿子).”** This illustrates the high priority the CCP places on propaganda work.

To this day, the **CCP has established a comprehensive propaganda system:** The Central Leading Group for Propaganda, Ideological, and Cultural Work (中央宣傳思想文化工作領導小組) was established within the Central Committee, **headed by Cai Qi, a member of the Politburo Standing Committee** responsible for ideological work.

The decisions made by the Leading Group are coordinated by the Central Committee’s Propaganda Department (中宣部), which directs the various ministries and commissions in their implementation. Relevant units include:

- the Cyberspace Administration of China (網信辦)
- the State Administration of Radio, Film, and Television (廣電總局)
- the State Administration of Press and Publication (新聞出版署)
- the Ministry of Culture and Tourism (文化和旅遊部)

- the Information Office of the State Council (國務院新聞辦公室)
- the Information Office of the Ministry of National Defense (國防部新聞局).

For more information, see: Investigation Bureau of the Ministry of Justice, ed., Overview of Mainland China – 2023 Edition, p. 117, Taiwan, Taipei.

Based on relevant documents published by the CCP in recent years, speeches by the leadership, and practical experience, several characteristics of the CCP's propaganda work can be summarized.

These are:

- Politically, the principle applies: **“centralized decision-making, but local implementation”**;
- In administration, the application of the **“Central Kitchen”** (中央廚房) model, which is the central catchphrase for the approach of the single-party system focused on central control.

The CCP believes that propaganda work is not merely a matter for the top echelons but relies on the cooperation of local governments at all levels to build a comprehensive media ecosystem. **To encourage local governments to participate, the Party acts as the driving force; the evaluation and review (評估考核) of local governments must be strengthened so that they implement the central government's policies in a coordinated manner.**

Under strong pressure from the CCP Central Government (中共中央政府), local

governments have followed suit. Currently, nearly all propaganda departments from the central to the local level are represented on new media platforms such as “WeChat” (微信), “Jinri Toutiao” (今日頭條), and “Douyin” (TikTok, 抖音).

Through the integration of internet networks, traditional media, and new media, vast amounts of information about daily life and citizen-friendly services are disseminated to achieve the propaganda objectives (眾宣傳目的) of exerting influence.

c) The “central kitchen” (中央廚房) model applied in management refers to the fact that traditional media must develop various forms of transmission in the age of multimedia diversification.

Regardless of how much the forms change, existing media will continue to play the role of a “central kitchen” and serve as the core for decisions regarding the development forms and reporting content of various media, ensuring that the various new media do not deviate from the original intent of dissemination.

Let's take China's three major traditional media groups as an example:

- The **“People's Daily”** (人民日報) operates a “central editorial office” as its decision-making hub; in addition, there is the Chinese-language online platform **“People's Daily Online”** (人民網), the English-language online platform **“People's Daily”**, and public accounts or fan pages have been

set up on instant messaging apps such as **“WeChat”** (微信), **“Twitter”** (推特), **“Facebook”** (臉書), and the short-video platform **“Douyin”** (TikTok, 抖音), each of which has public accounts or fan pages.

- **“Xinhua News Agency”** (新華社) has a **“Global Reporting Platform”** (全球報導平台) as its decision-making hub; in addition, there is the Chinese online platform **“Xinhua Net”** (新華網), the English online platform **“Xinhuanet,”** as well as public accounts or **fan pages** on other instant messaging apps and short-video platforms.
- **“China Central Television”** (CCTV, 中央電視台) has an **“Integrated Media Editorial Department”** (融媒體編輯部) as its decision-making hub; in addition, there is the Chinese online platform **“CCTV News”** (央視網), the English on-

line platform “CCTV,” as well as public accounts or **fan pages** on other instant messaging and short-video platforms.

In summary, the “central kitchen” model ensures that, under the same parent company, news research, editorial reporting, content, and the configuration of reporting formats are well-coordinated for each subsidiary media outlet. This ensures that, on the one hand, the subsidiary media outlets do not “fight their own battles” (各自為戰) and, on the other hand, that reporting overlaps between the individual subsidiary media outlets are avoided as much as possible. Please refer to the following table for a detailed breakdown of responsibilities.

6.8. Structure of the CCP’s Working System for Propaganda Directed at Taiwan and Abroad

a) Leading Group and Coordination Group (Decision-making System)

Table VI–1

Level	Unit	Function
Central	CCP Central Leading Group for Taiwan Affairs (中共中央對臺工作領導小組) Xi Jinping serves as head	Coordination and direction of major decisions regarding Taiwan; effectively the highest center of power
Ministries	Leadership (Coordination) Group for Taiwan Affairs of the Ministries (部委對臺工作領導、協調小組)	Composed of several ministries of the State Council with a strong focus on Taiwan affairs

Level	Unit	Function
Local	Leadership (Coordination) Groups for Taiwan Affairs of Party Committees at Various Local Levels (地方各級黨委對臺工作領導小組)	The heads are usually appointed from among the deputy secretaries of the local Party committees
Coordinating bodies	Unified Front Work Departments at the central and local levels (中央、地方各級統戰部)	Primarily responsible for the united front (統戰) and ideological infiltration (思想滲透) regarding Taiwan

b) TAO* System (Policy Implementation System, 臺辦系統, 政策執行系統)

Level	Unit	Function
Central (Party/ State Council)	Taiwan Affairs Office of the Central Committee (中臺辦) / Taiwan Affairs Office of the State Council (國臺辦) (Central TAO)	“One apparatus, two names”; responsible for implementing Taiwan policy
Local	Provincial, municipal, county, and district offices for Taiwan affairs (省臺辦、地市臺辦、縣區臺辦)	Responsible for implementing local Taiwan policy
Ministries	Department of Hong Kong, Macao, and Taiwan Affairs of the Ministry of Foreign Affairs; Department of Taiwan, Hong Kong, and Macao Affairs of the Ministry of Commerce; Department of Cultural Affairs in Hong Kong, Macao, and Taiwan of the Ministry of Culture (外交部港澳臺司、商務部臺港澳司、文化部港澳臺文化事務司)	Special working units for Taiwan affairs within the ministries
ARATS	Association for Relations Across the Taiwan Straits (海峽兩岸關係協會, 海協會)	Counterpart to Taiwan’s SEF (海基會)

**Note: TAO stands for Taiwan Affairs Office of the State Council (PRC) = 國務院台灣事務辦公室. The counterpart is the Mainland Affairs Council (MAC) = 陸委會 – Dalu Wei Yuanhui. Semi-official contacts in Taiwan are handled by the SEF – Straits Exchange Foundation = 海基會 and in China by the ARATS = 海協會, 海峽兩岸關係協會/ Association for Relations Across the Taiwan Straits.*

*Taiwan: **MAC** (陸委會) → Policy, Strategy / **SEF** (海基會) → Talks & Agreements.*

*China: **TAO** (國台辦) → Policy, red lines / **ARATS** (海協會) → Talks & technical agreements, 海峽兩岸關係協會.*

c) Intelligence Gathering System (情資蒐集系統)

Unit	Function
TAO System (臺辦系統)	TAO Research Institute, Research Center for Cross-Strait Relations, research departments of local TAOs, Taiwan research departments in various ministries
News System (新聞系統)	Official media outlets such as Xinhua News Agency (新華社), People's Daily (人民日報), CCTV (中央電視臺), China News Service (中國新聞社), and China Review News (中國評論通訊社)
Military Intelligence System (軍情系統)	Intelligence Bureau of the Joint General Staff of the Central Military Commission, Liaison Department of the Political Work Department, 6th Office of the Network Warfare Department of the Strategic Support Force (responsible for cyber forces)
National Security System (國安系統)	Ministry of State Security (MSS) and its local branches at various levels, Ministry of Public Security (MPS) and its local branches at various levels
United Front System (統戰系統)	Central and local departments for united front work, united front departments of various organizations and groups
Consultative and Research System (諮詢研究系統)	Divided into official agencies, universities, and civilian think tanks, such as the Institute for Taiwan Studies of the Chinese Academy of Social Sciences, the Institute for Taiwan Studies of Xiamen University, the Institute for Taiwan Studies of Shanghai University, the China Institutes of Contemporary International Relations (CICIR), the Shanghai Institutes for International Studies, etc.

d) System of Political Parties and Civil Society Organizations (政黨與民間社團系統)

Unit	Function
Political Party System (政黨系統)	Taiwan-related parties, such as the Taiwan Democratic Self-Government League (臺盟), the Kuomintang Revolutionary Committee (民革), etc.
System of civil society organizations (民間社團系統)	All-China Federation of Taiwan Compatriots (全國臺灣同胞聯誼會), Whampoa Military Academy Alumni Association (黃埔軍校同學會), China Council for the Promotion of Peaceful National Reunification (中國和平統一促進會), China Overseas Friendship Association (中華海外聯絡會), China Mazu Culture Exchange Association (中華媽祖文化交流協會), etc.
System of Taiwanese Businesspeople (臺商系統)	Associations of Taiwanese-invested enterprises in various regions (Taiwan Business Association, 臺商協會), the National Federation of Associations of Taiwanese-Invested Enterprises (全國及各地臺胞投資企業聯誼會, 臺企聯)

e) United Front System (統戰系統)

Unit	Function
Central (中央)	3rd Bureau (Bureau for United Front Work in Hong Kong, Macau, and Taiwan) of the United Front Work Department of the Central Committee (中央統戰部港澳臺統戰工作局 (第三局))
Local (地方)	United Front Work Departments at various local levels (地方各級統戰部門)
Political Consultative Conference (CPPCC system)	National Committee of the Chinese People's Political Consultative Conference (全國政協), local Political Consultative Conferences at various levels (地方各級政協)

f) Military System (軍方系統)

Unit	Function
Central Military Commission (中央軍委)	Intelligence Bureau of the Joint General Staff (聯合參謀部情報局), Liaison Bureau of the Political Work Department (政治工作部聯絡局)
Strategic Support Force (戰略支援部隊)	6th Bureau of the Department of Cyber Warfare (網絡空間作戰部第六局)



NEW STRUCTURE OF THE PLA SERVICES

Four Major Services

Army
Navy
Air Force
Rocket Force

Four Independent Branches

Military Aerospace Force
Cyberspace Force
Information Support Force
Joint Logistic Support Force

Source: Training material from an intelligence agency of the Republic of China (ROC) in Taiwan.

g) Propaganda System (宣傳系統)

Unit	Function
Central (中央)	Central Leading Group for Propaganda and Ideological Work (中央宣傳工作思想小組), Propaganda Department of the Central Committee (中央宣傳部)
Local (地方)	Propaganda departments at various levels (各級宣傳部門)
Official media (官方媒體)	News agencies: Xinhua News Agency (新華社), China News Service (中國新聞社); Newspapers: People's Daily (人民日報), Hong Kong Wen Wei Po (香港文匯報), Ta Kung Pao (大公報), etc.; Radio: China National Radio (中央人民廣播電臺), Voice of the Strait (海峽之聲廣播電臺), etc.

Unit	Function
	Television: China Central Television (CCTV), various provincial and municipal satellite TV stations, etc.
	Magazines: China Review (中國評論), Voice of Taiwan (臺聲), Cross-Strait Relations (兩岸關係), etc.
	Film: China Film Group Corporation (中國電影發行放映公司), etc.
	Publishers: Jiuzhou Press (九州出版社), etc.
New Media and Influencers (Self-Media) (新媒體與自媒體網紅)	Methods of infiltration targeting Taiwanese youth and civil society groups (such as Xiaohongshu (小紅書), Douyin (TikTok), Weibo (微博))

h) Taiwan-related work at the local level (promoting integrated development)

(地方層級對臺工作, 推動融合發展)

Unit	Function
Fujian Province (福建省)	Strait West Coast Economic Zone (海峽西岸經濟區), Pingtan Comprehensive Pilot Zone (平潭綜合實驗區), Kinmen-Xiamen Cross-Strait Integrated Development Demonstration Zone (金廈兩岸融合示範區)
Various Provinces (各省)	Shanghai Free Trade Zone (上海自由貿易區), Taiwanese Youth Entrepreneurship Parks in various provinces (各省臺灣青年創業園區), Taiwanese Compatriots' Home (臺青之家)

Note: The "Kansai Airport Incident" (關西機場事件) refers to a controversy in September 2018 after Typhoon Jebi paralyzed Kansai International Airport, leaving thousands of travelers stranded. Claims spread on social media that the Chinese consulate had sent buses to evacuate Chinese citizens and only those Taiwanese travelers who identified themselves as "Chinese." This account later proved to be largely disinformation and sparked a political debate in Taiwan about influence operations and "fake news." Source: Central News Agency (CNA), "Yomiuri Reviews Kansai Airport Incident: Taiwan Faces Fake News Crisis," Oct. 6, 2018; and Taipei Times, "Chinese Kansai Evacuation Story 'Fake News': DPP," Sept. 9, 2018. https://www.taipeitimes.com/News/taiwan/archives/2018/09/09/2003700087?utm_source=chatgpt.com. Accessed March 12, 2026, at 12:10 p.m.

Chapter 7 – Analysis of Chinese Espionage Activities. Have 5,000 or 100,000 Chinese Agents Infiltrated Taiwan?

7.1. Definition and Distinction: United Front vs. Espionage

To adequately assess the threat posed to Taiwan by the People's Republic of China (PRC), a precise terminological distinction between United Front work and traditional espionage is essential. **United Front work is primarily aimed at influencing civil society and ideological infiltration.** Its range of targets is broad and extends far beyond the circle of those holding classified information. Activities often take place in the legal or semi-legal sphere—for example, through cultural exchanges, religious programs, or economic cooperation.⁴³

In contrast, **espionage is defined** as a covert, **targeted activity explicitly aimed at stealing state secrets or sabotaging critical infrastructure.** While the united front openly promotes “identification,” espionage operates in secret, using financial incentives or blackmail and focusing on individuals with access to classified information and access to secret and confidential materials.⁴⁴

However, there is a **sybiotic relationship: the united front often serves as a legal cover network in which potential agents are identified, vetted, and recruited. Espionage thus utilizes the structures of the united front as an operational precursor.**⁴⁵

7.2. The Debate Over Quantifying Infiltration

A central point of contention in Taiwan's national security debate is the actual number of Chinese actors on the island.

a) The Baseline Estimate: 5,000 Agents

The figure of 5,000 agents is often regarded by experts as a conservative lower limit. As early as 2007, former Deputy Minister of National Defense **Lin Chung-pin** (林中斌) referred to this order of magnitude.⁴⁶ **Recent analyses by former military intelligence chief Liu Te-liang** (劉德良) **confirm that this number must have been far exceeded.** These actors are deeply embedded in government agencies, private companies, and civil society organizations.⁴⁷ The National Security Bureau supplements this perspective with internal data, according to which, among other things, **1,332 PRC citizens reported missing in Taiwan are factored into potential risk assessments.**⁴⁸

b) Historical Development and Unreported Cases

As early as 2000, the then-deputy director of the NSB, **Han Kun** (韓鯤), pointed out that **among the 540,000 annual visitors from the PRC, at least 3,000 individuals held the status of intelligence operatives.**⁴⁹

Eighteen years later, it is estimated that the number of infiltrated and “sleeper” agents far exceeds 5,000. Since Chinese intelligence services operate according to the principle of isolated cells and double coverage, it can be assumed that even the adversary cannot provide an absolute total figure.⁵⁰

c) Groups of Actors and Infiltration Channels

Of the 159 individuals charged with espionage since 2020, 60% are active or retired military personnel (52 active-duty soldiers, 43 veterans).⁵¹ Particularly alarming are successful infiltrations within the political landscape, extending to the immediate vicinity of the highest state offices (including former assistants to the President, Speaker of the Legislative Yuan, and advisors to the Office of the President).⁵² **In addition to organized crime and shell companies, “social gathering places” are identified as primary channels where contacts are initiated through financial or sexual enticement.**⁵³

7.3. Analysis of Cognitive Warfare: The NSB Annual Report 2025

In addition to the physical presence of agents, the latest annual report from the **National Security Bureau of the Republic of China (ROC) in Taiwan (National Security Bureau, 中華民國國家安全局)**, hereinafter referred to as the NSB, documents a massive expansion of cognitive warfare against Taiwan. This January 2026 report provides a detailed analysis of the People’s

Republic of China’s strategies in 2025.⁵⁴

a) Strategic Objectives and Networks of Actors

The NSB notes that the PRC specifically employs cognitive operations to exploit current events in Taiwan. The **primary objectives** are to “**exacerbate internal divisions in Taiwan,**” “**weaken the Taiwanese population’s will to resist the enemy,**” “**influence the willingness of allies to support Taiwan,**” and “**gain support for China’s position**” (identity politics).⁵⁵

This involves a highly coordinated system. After narrative themes are established by the party leadership, state and military systems mobilize a multitude of collaborating organizations. These include specialized IT companies, marketing firms, and so-called “Internet Water Army Groups (網絡水軍集團),” which systematically spread disinformation.⁵⁶

b) The Five Main Tactics of Cognitive Manipulation

During the reporting period, the NSB identified five key tactics used by the PRC to manipulate the Taiwanese public:

1. **Data-driven analysis of social dynamics:** The MSS and the Cyberspace Administration of China (CAC) use **big data to identify trends and vulnerabilities in Taiwanese society.** The goal is to tailor narrative themes so precisely that they generate maximum resonance and division.⁵⁷

2. **Multi-channel infiltration: Disinformation** is **disseminated** across a variety of platforms, with PRC state media, social networks, and local platforms in Taiwan being utilized simultaneously to create an apparent consistency in the narratives.⁵⁸
3. **AI-powered scaling:** Through the use of artificial intelligence, content (text, videos, deepfakes) is produced in massive quantities. **In 2025 alone, the NSB identified over 4 million suspicious posts that fell into the disinformation category.**⁵⁹
4. **Use of local influencers:** The PRC utilizes collaborative organizations and **opinion leaders within Taiwan** to “localize” narratives and make them appear more credible.
5. **Timing and event-hopping:** Current crises or **political debates in Taiwan are seized upon within hours to reinterpret them in line with the PRC’s interests** and destabilize public discourse.⁶⁰

7.4. Response Mechanisms and International Cooperation

The NSB has responded to this threat with an integrated reporting and response system. Over 3,200 critical disinformation

campaigns were reported directly to the relevant government agencies in 2025 to enable real-time countermeasures. A key component of the defense is collaboration with civil society fact-checkers and platform operators to flag or remove manipulative content.⁶¹

The international dimension deserves special mention. **According to the NSB, Taiwan serves as a “frontline state” against cognitive warfare.** Consequently, **over 80 security dialogues and intelligence conferences were held with international partners (including the U.S., the EU, and Australia) in 2025. The goal is to build a “democratic network” to jointly combat information manipulation by totalitarian regimes.**⁶²

7.5. The Economics of Espionage and Conclusion

Intelligence operations are extremely cost-effective compared to conventional warfare. While China’s budget for this has grown massively, Taiwan’s budget is under pressure from public demands for transparency.⁶³ **According to the NSB effective defense therefore requires a hybrid strategy that prioritizes the protection of physical institutions, the monitoring of united front structures, and the defense of the digital information space in equal measure.**

Chapter 8 – Religious Infiltration and the “Iron Triangle” – The Instrumentalization of Mazu Worship and Organized Crime

8.1. The United Front and the “Soft Power” of the Sea Goddess

Chinese united front work (統一戰線工作) places particular emphasis on Taiwan’s cultural and religious identity. The National Security Bureau (國家安全局) and international observers note an increasing instrumentalization of the sea goddess Mazu (媽祖), the island’s most popular deity. **The Chinese Communist Party (CCP) uses the veneration of Mazu as “soft power” to construct a shared cultural identity across the Taiwan Strait and thus subtly undermine Taiwan’s democratic foundations.**⁶⁴ Religious practice is thus reinterpreted as a political tool that presents “reunification” (統一) as the natural consequence of a shared tradition.

8.2. The “Iron Triangle”: Temples, Gangs, and the CCP

Infiltration occurs through a complex network referred to in expert circles as the “Iron Triangle” (鐵三角). **This consists of cooperation between Taiwanese gangs (organized crime, 有組織犯罪), local Mazu temples, and the CCP’s United Front Work Department.**⁶⁵ This alliance enables Beijing to exert influence down into the deepest local structures of Taiwanese society, which are often difficult for state security agencies to access.

8.3. The Role of Organized Crime: The Bamboo Union

The “Bamboo Union” (竹聯幫), one of Taiwan’s most powerful criminal organizations with close ties to the mainland, plays a central role in this network. Gangs often act as intermediaries for the United Front. They infiltrate temple boards and use their social authority to spread political narratives or support pro-China candidates at the local level.⁶⁶ The connection between crime and religion offers Beijing an ideal platform for covert operations (秘密行動) under the guise of faith.

8.4. Institutional Hijacking: The Case of the Dajia Jenn Lann Temple

A prominent example of this form of institutional influence is the Dajia Jenn Lann Temple (大甲鎮瀾宮). By controlling influential religious institutions, the United Front can shape the discourse during the major Mazu pilgrimages, which 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 political messages from the CCP.⁶⁷

8.5. The “Taiwan Mazu Fellowship Association” as a Network

To systematize this infiltration, organizations such as the Mazu Fellowship were established. These associations serve as a formal structure for religious exchange but function de facto as channels for United Front work. They facilitate coordination between hundreds of temples in Taiwan and their “mother temples” in China (particularly in Meizhou), thereby establishing a permanent flow of influence.⁶⁸

8.6. Financial Dependencies and Money Laundering

The infiltration of religious organizations also offers opportunities to circumvent financial controls. Since temples in Taiwan often have access to substantial, sometimes opaque, donations, they can serve as channels for “black money” from China. This money is used to finance political activities or to bribe local officials, with the gangs’ criminal networks handling the money laundering.⁶⁹

8.7. The Tianjin Binhai Mazu Cultural Park

On the Chinese side, monumental projects such as the “Tianjin Binhai Mazu Cultural Park” (天津濱海媽祖文化) are being built to portray Taiwan as a religious periphery of China. These centers serve as backdrops for political forums to which Taiwanese temple leaders and local politicians are invited. The goal is to cultivate a loyal elite within the Taiwanese religious community that represents Beijing’s interests.⁷⁰

8.8. Threat to the Substance of Democracy

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. This creates a safe space in which the United Front can carry out its activities largely unhindered. The report warns that the “instrumental use of Mazu” will, in the long term, alter public perception in such a way that Taiwan’s political autonomy appears as an unnatural deviation from cultural unity.⁷¹

8.9. Security Implications

The connection between gangs and temples poses a hybrid threat. In the event of a conflict, these networks could be used to incite social unrest, carry out acts of sabotage, or hinder mobilization. Even in peacetime, the criminal structures of the Bamboo Union provide Beijing with a “fifth column” that can be activated at any time to carry out destabilizing actions.⁷²

8.10. Summary: The Need for a Holistic Defense

In summary, the defense against Chinese infiltration must not end with the surveillance of the military and government. The example of Mazu worship shows that Taiwan’s national security is inextricably linked to the resilience of its civil society and the transparency of its religious institutions. An effective strategy must therefore include raising awareness about the “Iron Triangle” and strengthening the independence of local temples against criminal and political influence.⁷³

Chapter 9 – The Political Turn of 2025: President Lai's Security Agenda and the New Wave of Legislation

9.1. From Restraint to a Defensive Democracy

For a long time, it seemed as though the Taiwanese government was not confronting the hybrid threats posed by the People's Republic of China (中華人民共和國) with the necessary resolve. Critics such as former intelligence chief **Liu Te-liang** (劉德良) pointed out that treason was sometimes punished more leniently than simple theft, and that the number of espionage cases was rising sharply. Existing laws, such as the Anti-Infiltration Act (反滲透法), were considered too narrowly defined to counter modern influence operations carried out through front companies and online networks. **This changed fundamentally in 2025, when the government under President Lai Ching-te declared national security a top priority.**⁷⁴

9.2. The President's Speech as a Milestone (March 13, 2025)

Following a meeting of the high-level National Security Council (國家安全會議), **President Lai delivered a keynote address that is regarded as a strategic milestone for the defense of Taiwanese democracy.** In it, he addressed “spiritual and psychological warfare” as a central threat to the state's survival.

a) China Uses “Spiritual and Psychological Warfare”

Lai issued a stark warning about how Chinese state media uses narratives to stir up internal opposition in Taiwan. These messages are rapidly disseminated through specific channels, with individuals literally making careers out of producing “United Front” content. The goal is to spread the message that democracy is useless and to foster skepticism toward the U.S. and Taiwan's own military in order to sow division and opposition.

b) Incorporating international expertise on “psychological warfare”

To underscore the scientific and strategic dimensions of this threat, President Lai quoted the military expert Kerry K. Gershaneck:

“...renowned strategic scholar Kerry K. Gershaneck stated that China plans 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. What they are trying to do is sow seeds of discord in our society...”

Lai thus directly incorporated the concept of psychological warfare into the national

context: China is attempting to weaken society from within and sow the seeds of discord through coordinated media and information strategies.

c) China as a “Foreign Hostile Force”

The speech represents a legal U-turn **because it marks the first time a Taiwanese government official has referred to China as a hostile power:**

“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.”

This designation as a “foreign hostile actor” **created the necessary legal basis for intensified countermeasures in the areas of counter-influence and information security.**

d) Detailed Description of Infiltration Tactics

In his analysis, President Lai cited several concrete examples to illustrate the extent of Chinese infiltration:

- **Media infiltration:** Targeted influence operations or recruitment of active and former military personnel to raise questions of loyalty and conduct espionage.

- **Media infiltration:** Systematic influence on media outlets, political commentators, artists, and influential social groups.

- **Propaganda networks:** The use of Chinese state media in combination with “co-opted” local actors to massively disseminate divisive information.

- **Identity-based manipulation:** The use of economic and social inducements aimed at confusing the national identity of Taiwanese people and fostering a creeping acceptance of Beijing’s positions.

9.3. Appeal to the Population and Civil Resilience

As a result, Lai called on the entire population to become part of the national defense. He appealed to citizens:

- To significantly strengthen their own **media literacy** in order to recognize disinformation
- To actively engage in **civic participation** and information awareness
- To promptly **expose** coordinated influence or propaganda campaigns
- Strictly avoid activities that could harm **national interests**

This underscores Lai’s view that cognitive resilience is an integral part of modern national defense.

9.4. The Opposition's Response: Criticism and Obstruction

The announced tightening of security laws sparked fierce resistance. **The Kuomintang (KMT) under Eric Chu (朱立倫) and the Taiwan People's Party (TPP, 台灣民眾黨) accused the government of fostering an "atmosphere of fear" to stigmatize political opponents.**

These tensions led to a deep parliamentary crisis:

- **Boycott of security briefings:** In **June 2025**, **Eric Chu** and **Huang Kuo-chang (黃國昌)** **declined invitations to national security briefings at the Office of the President**, arguing that the closed-door format lacked transparency.
- **Budget blockade:** The opposition used its majority in the Legislative Yuan (立法院) to block key defense budgets and special budgets aimed at strengthening resilience in the procedural committee.

9.5. The Legislative Offensive (September 2025)

Despite the resistance, Lai stepped up the pace in the fall. **On September 12, 2025**, he announced **a massive wave of legislation**. Based on 17 national security strategies, over **a hundred legislative amendments** are to be introduced.

In doing so, Lai defined the **"Four Key Elements for Protecting Taiwan"** (守護台灣的四大要素):

1. **Cultural Identity** (文化認同): Strengthening national self-confidence against Beijing's narratives.
2. **Democratic institutions** (民主體制): Safeguarding political processes against manipulation.
3. **Economic strength** (經濟實力): Utilizing technological capabilities as a protective barrier and strengthening industry through special budgets.
4. **Sound social systems** (健全社會制度): Stable institutions as a bulwark against China's authoritarian model.

9.6. Conclusion

The year **2025 marks Taiwan's transition to a "defensive democracy."** Through his speech in March and the subsequent wave of legislation, President Lai has made it clear that cognitive and psychological warfare are treated as existential threats. **While the government is closing legal loopholes, internal political division—exacerbated by the opposition's obstructionist stance—remains the greatest challenge to the implementation of this new security architecture.**

Note: All quotations in this chapter are taken from President Lai's speech.

Chapter 10 – Strategic Paralysis: The “Fifth Column” and the Erosion of Parliamentary Stability

10.1. The Artificial Crisis

President Lai Ching-te’s speech seemed to come at just the right time, as the rifts in Taiwanese society have increased alarmingly this year. **What may appear on the surface to be a lively democratic discourse turns out, upon closer analysis, to be 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.⁷⁵

10.2. The Parliamentary Blockade: Defense in the Crosshairs

A central arena for this destabilization is the Legislative Yuan (立法院). **Since President Lai took office, the opposition—comprising the Kuomintang (中國國民黨 – KMT) and the Taiwan People’s Party (台灣民眾黨 – TPP)—has used its majority not to engage in constructive lawmaking, but to systematically block national security interests.** This is particularly evident in the special defense budget of 1.25 trillion NT\$. While the government is pursuing a comprehensive strategy for asymmetric warfare, the opposition is persistently blocking this budget in the Rules Committee.⁷⁶

The TPP, under its caucus leader Huang Kuo-chang, instead introduced its own

draft, which, however, according to experts at the Ministry of National Defense, is strategically flawed and deliberately omits essential elements of U.S. cooperation—such as software for tactical networks and spare parts for helicopters.⁷⁷ **This selective budgeting jeopardizes the sustainability of Taiwan’s combat readiness and hinders joint operations with allies.**

10.3. The Role of the KMT and Willy Lam’s Analysis

Critics see this behavior as direct manipulation by Beijing. Renowned China expert **Willy Lam** (林和立) offers a stark assessment of the situation. Lam states: **“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 (中國共產黨).** There is a widespread view that the KMT has essentially been ‘bought’ to politically neutralize Taiwan from within.” **Speaking** at an event before the Taiwan Foreign Correspondents’ Club (TFCC), **the former China editor of the South China Morning Post said: “A large part of the KMT appears to already be controlled by the CCP.”** The KMT is thus increasingly acting as an extension of a power that seeks a defenseless Taiwan by weakening the nation’s defense capabilities at precisely

the moment when external threats are escalating dramatically.

10.4. Radicalization in Personnel Policy: Cheng Li-wun and Han Kuo-yu

The KMT's personnel reshuffle underscores this change of course. The new chairwoman, **Cheng Li-wun** (鄭麗文), has also caused a stir with decidedly pro-China narratives that increasingly call Taiwan's sovereignty into question. This course is flanked by Parliament Speaker **Han Kuo-yu** (韓國瑜), who has already sparked controversy in the past due to his closeness to representatives of the Beijing Liaison Office in Hong Kong. Under their leadership, the KMT has evolved from a statesmanlike opposition into a force that physically and procedurally blocks the legislature to prevent constitutional decisions—such as the appointment of new Supreme Court justices.⁷⁸

10.5. Personnel Infiltration: The Case of Lee Chen-hsiu and the “Zhongpai”

In addition to the political sphere, social infiltration is coming into focus. A first in Taiwanese parliamentary history is the TPP's attempt to bring **Lee Chen-hsiu** (李貞秀), a person born in China who has not officially renounced his citizenship of the People's Republic, into parliament.⁷⁹ This raises significant constitutional questions, as the law prohibits individuals with dual citizenship from holding high public office.

This personnel matter is part of the phenomenon known as “Zhongpei” (中配)—Chinese wives of Taiwanese citizens, some of whom are deliberately exploited as agents of influence. In early 2025, several “red bloggers” who were spreading pro-China propaganda from Taiwan were deported.⁸⁰ The KMT's prompt criticism of these deportations illustrates just how much the opposition is already functioning as a shield for Beijing's influence operations.

10.6. The United Front Network: The Jamestown Analysis

The latest report by the Jamestown Foundation on the activities of the United Front confirms this finding. Beijing has intensified its efforts not only to co-opt elites but also to influence Taiwanese civil society directly through social media and migrant networks.⁸¹ The strategy aims to undermine the government's ability to govern by creating “chaos from within,” so that military intervention would encounter less resistance in the event of an emergency.

10.7. Conclusion

The synergy of parliamentary deadlock, obstruction of the judiciary, and personnel infiltration points to a master plan devised in Beijing. Taiwan faces not only an external military threat but also an existential test of its democratic institutions, which is being consistently driven forward by internal actors—aided by a “bought” opposition.⁸²

Chapter 11 – The “Japan Crisis” – Geopolitical Escalation and Cognitive Synchronization

11.1. The “Taiwan Incident” as an Existential Crisis

In late 2025, the Communist Party of China massively expanded its arsenal of hybrid warfare to target Japan. The trigger was a statement by Japanese Prime Minister **Sanae Takaichi** (高市早苗) during a session of the House of Representatives on November 7, 2025. **Takaichi officially designated a potential “incident in Taiwan” (台灣有事) as an “existential crisis situation” (存立危機事態) for Japan.**⁸³

Beijing’s reaction was immediate and unusually sharp. The (then) Chinese Consul General in Osaka, **Xue Jian** (薛劍), posted a “decapitating” remark on Twitter that caused worldwide outrage and brought diplomatic relations to a low point.⁸⁴

Note: Xue wrote: “那種擅自闖入的骯髒頭顱，就該毫不猶豫斬掉。你們做好覺悟了嗎？” The correct translation is as follows: “Those filthy heads that dare to intrude without permission should be cut off without hesitation. Are you prepared for the consequences?”

11.2. Hybrid Threats: The Multi-dimensional Escalation

Starting in mid-November 2025, the CCP launched a coordinated campaign that went far beyond verbal threats and encompassed cognitive, diplomatic, military, and economic dimensions.⁸⁵

- **Propaganda offensive:** State-run media outlets such as the Global Times (環球時報) and the Taiwan Affairs Office (國務院台灣事務辦公室) published a series of statements that culminated in an editorial in the People’s Daily (人民日報). **The editorial made it clear that Takaichi’s “provocative transgression” would not be tolerated under any circumstances.**⁸⁶
- **Economic and military pressure:** Beijing issued **travel warnings for Japan, announced naval exercises in the Yellow Sea, and completely halted imports of Japanese seafood** on November 19.⁸⁷
- **Symbolic politics and “panda diplomacy”:** Even the cooperation regarding the giant pandas at Ueno Zoo was exploited. The Chinese media declared the early return of the animals in December 2025 to be the end of an era, as Japan had repeatedly crossed “red lines.”⁸⁸

11.3. Cognitive Synchronization: The Alliance of Narratives

According to the Taiwan Information Environment Research Center (IORG), a particularly concerning development in

2025 was the **increasing synchronization of narratives between the CCP and the Taiwanese opposition parties, the Kuo-mintang and the Taiwan People's Party.**⁸⁹

Within the Chinese-language information space, these actors jointly shaped an alternative worldview:

1. **Historical Stigmatization:** The **three parties deliberately emphasized Japan's connection to its wartime history** and used terms such as “militarism” (軍國主義), “far-right,” and “warmon-gering” (窮兵黷武) to discredit Prime Minister Takaichi and the alliance with Taiwan.⁹⁰
2. **The “Destruction of Taiwan” Narrative:** In a striking division of labor, Japan was positioned as an “aggressor” and “disturber of peace.” The KMT criticized Japan's alleged “pandering” to the U.S., while TPP spokespeople suggested that Japan's stance was merely directed by Washington.⁹¹
3. **Undermining sovereignty:** Prominent KMT figures supported Beijing's false premise that the Taiwan Strait is purely an “internal matter” of China. Statements by **Ma Ying-jeou** (馬英九), **Hung Hsiu-chu** (洪秀柱), and Representative **Kao Chin-su-mei** (高金素梅)—such as that the Taiwan Strait “is none of the

Japanese's business”—de facto undermined the Republic of China's international position.⁹²

11.4. Defamation of the Lai Administration

In parallel with the attack on Japan, the CCP and the Taiwanese opposition coordinated a smear campaign against President Lai Ching-te. Lai was accused of behaving “submissively” toward Japan (媚日) and cultivating “colonial ties” to advance independence. **The CCP used vulgar metaphors such as “wagging one's tail to show loyalty,” while Taiwanese politicians like Su Ching-chuan** (蘇清泉) **claimed that Japan's military inaction during Chinese maneuvers proved the unreliability of its allies.**⁹³

11.5. Conclusion

Events at the end of 2025 show that Beijing's cognitive warfare no longer stops at national borders. **The targeted destruction of the image of allies such as Japan through information manipulation, coupled with the Taiwanese opposition's adoption of these narratives, is weakening the democratic alliance from within.** The IORG warns that this “toxic content” is flooding public forums and undermining the foundations of Taiwanese democracy as well as trust between partners.⁹⁴

Chapter 12 – Specific Espionage Cases and Their Criminal Consequences

12.1. The Judiciary in the Fight Against Infiltration (2025–2026)

The year 2025 marked a turning point in Taiwanese legal history regarding the prosecution of espionage and subversive activities. Faced with a massive increase in investigations—according to security authorities, case numbers had been rising steadily since 2022—the government under President Lai Ching-te responded by tightening judicial practices. **A central feature of this period is the end of the era of “lenient sentences” and the consistent application of the reformed “National Security Act.”** Due to the high involvement of military personnel in espionage cases (approx. 66%), efforts to reestablish special military courts are also being pursued.⁹⁵

12.2. Final Convictions (Spies and Collaborators)

This section lists the cases in which the Taiwanese judiciary (particularly the Supreme Court) handed down final judgments in 2025 or early 2026:

- **The case of the “Rehabilitation Alliance Party” (January 2026):** Chairman **Qu Hongyi** (屈宏義) was sentenced to **10 years in prison** by the Supreme Court in the final instance. He had recruited retired officers on behalf of

the PLA to form an “internal force” and transmit strategic coordinates (including those from the AIT). Six other cadres received prison sentences ranging from 3.5 to 8.5 years.⁹⁶

- **Military espionage in the presidential security sector (March/December 2025):** On December 5, 2025, the Supreme Court upheld the prison sentences against three former military personnel from the “Presidential Office Security Unit.” The sentences of up to **7 years in prison** for passing on sensitive information are thus final.⁹⁷
- **The Shih Chun-cheng Case (August 2025):** On August 21, 2025, the Supreme Court upheld the verdict against former Air Force officer **Shih Chun-cheng** (史濬程). He was sentenced to **2 years and 2 months in prison** for violating the National Security Act.⁹⁸
- **The former DPP officials’ cell (September 2025):** Four former DPP employees were convicted of espionage. They passed travel itineraries of government leaders on to Beijing. **Huang Chu-jung** (黃取榮) received the maximum sentence of **10 years in prison**; his accomplices were sentenced to terms ranging from 4 to 8 years.⁹⁹

- **The Diabolo Coach Case (June 2025):** **Lu Chi-hsien** (魯紀賢) was sentenced to **10 years and 6 months in prison**. He had built an extensive network that specifically recruited military and coast guard officers.¹⁰⁰
- **The CUPP Activities (March 2025):** Three members of the pro-Beijing Chinese Unification Promotion Party were convicted of illegally recruiting military personnel for Chinese interests. Their prison sentences became final over the course of the year.¹⁰¹

12.3. Ongoing Charges and Suspected Espionage Cases (as of March 2026)

- **The Ting Hsiao-hu network (November 2025):** Charges against seven individuals, including Chinese citizen **Ting Hsiao-hu** (丁小琥). He is alleged to have established a network under the guise of business trips that paid over 11 million NT\$ in bribes to active and retired officers (including Wang Wenhao and Tan Chun-ming).¹⁰²
- **Air Force Infiltration (March 2025):** Judicial authorities announced charges against two active-duty Air Force officers accused of passing military secrets to China.¹⁰³
- **Case of Reserve Officer “You” (November 2025):** Charges against a reserve captain suspected of selling military secrets to Chinese authorities via **Telegram**.¹⁰⁴

- **Peng Shun-fu** (彭順富), **March 2026:** A former employee of Taiwan’s National Security Bureau (NSB) was definitively sentenced to four years in prison by Taiwan’s Supreme Court on March 11, 2026.
- **Suspicious against media representatives:** Arrest of a journalist suspected of acting as an intermediary to bribe military personnel into disclosing classified information.¹⁰⁵

12.4. Summary Analysis of the Legal Basis

Judicial and prosecutorial practices in 2025 are primarily based on the following legal pillars:

1. **National Security Act** (國家安全法): The core instrument against the development of hostile organizations and espionage.¹⁰⁶
2. **Classified National Security Information Protection Act** (國家機密保護法): Specifically for the betrayal of state secrets by public officials.¹⁰⁷
3. **Anti-Infiltration Act** (反滲透法): Applied in cases of illegal political influence through foreign funds.¹⁰⁸
4. **Criminal Code of the Armed Forces** (陸海空軍刑法): Stricter penalties for active or former soldiers who betray military secrets.¹⁰⁹

12.5. Bibliography (Court Decisions & Primary Sources)

No.	Document Title / Case	Source	Official Link (Judgment/ Report)
1	Qu Hongyi (Rehabilitation Alliance) - 10 years in prison 統一戰線	CNA	Link
2	Supreme Court finalizes case involving former servicemen accused of espionage	Focus Taiwan	Link
3	Shih Chun-cheng's convictions under the National Security Act upheld/ 史濬程犯國安法部分罪名定讞 (Shih Chun-cheng)	CNA	Link
4	Taiwan convicts four former ruling party officials	The Guardian	Link
5	Sentence Lu Chi-hsien (Diabolo Network)	Focus Taiwan	Link
6	Seven charged with espionage (Ting Hsiao-hu)	Taipei Times	Link
7	2 Air Force officers indicted for espionage	AA News	Link
8	Reserve captain indicted (Telegram Case)	Taipei Times	Link
9	66% of Military Espionage Cases Involve the Armed Forces; President: Restore the Military Court System/ 國軍涉共諜案占比達 66%	Central News Agency (CNA)	Link
10	Reserve captain indicted for selling secrets via Telegram	Taiwan News	Link
11	Journalist detained over alleged military bribery	AP News	Link
12	Peng Shun-fu (彭順富), former agent of the National Security Bureau	Taipei Times	Link

Chapter 13 – Strategic Recommendations: The Defensible Republic

13.1. Introduction: Taiwan as the “Canary in the Coal Mine”

This study highlights a fundamental reality of security policy: The Republic of China (Taiwan) is today far more than a technological epicenter of the global microchip industry. Rather, the self-governed nation appears to be serving as a primary laboratory for a new, sinister form of 21st-century warfare.

On “Ilha Formosa,” Beijing is testing how a well-established democracy can be brought to implode from within through systemic infiltration, digital subversion, and psychological attrition. Anyone who underestimates this conflict as an isolated regional problem in the Western Pacific fails to recognize the global implications of China’s infiltration strategy. According to security experts, the campaign by the People’s Republic of China’s intelligence services is directed against the very foundations of those states that Beijing perceives as the “Western model of democracy.”

In this context, Taiwan acts as a geopolitical “canary in the coal mine.” 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—ranging from the exploitation of economic dependencies to**

cognitive warfare and the covert infiltration of spies and collaborators—serve as blueprints for future operations in Europe and North America.

For the Western community of values, Taiwan therefore offers not only a strategic early warning system but also an indispensable source of insights into the workings of modern hybrid influence operations. The following recommendations therefore address the government in Taipei as well as European security agencies and political institutions.

13.2. Paradigm Shift in Criminal Law: From Procedure to Resilience

The defense of open society must not end in legal paralysis. Democracies face the structural problem that their inherent openness is exploited by authoritarian actors as an operational vulnerability. Beijing deliberately exploits this weakness: **under the shield of liberal fundamental rights, the “fifth column” is deployed** to abolish that very freedom.

To counter this existential threat, Taiwan must complete the transition from a purely procedural rule of law to a consistent, robust legal order. **It is an absurdity in terms of security policy when treason and espionage are punished more leniently in judicial practice than ordinary property crimes.**

Particularly serious cases require draconian penalties—such as the disclosure of strategic defense plans or the active sabotage of national defense capabilities. To serve as an effective deterrent against high-ranking collaborators in the military and administration, these offenses should be punishable by life imprisonment even in peacetime. Incidentally, in the People's Republic of China itself, serious cases of treason and high treason can also be punished by the death penalty.

In parallel, robust emergency legislation modeled on international standards is required, such as that found in the German Basic Law. Should the legislature become incapacitated due to targeted obstruction or the influence of foreign powers, the executive branch must be temporarily authorized to make central security policy decisions by decree. **A state that loses its ability to act in the face of infiltration brings about its own downfall (Popper's Paradox).**

The alleged dismantling of the NSB's agent network in China—"HUMINT" (Human Intelligence), spies on the ground—during President Ma Ying-jeou's (2008–2016) term in office was a serious mistake.

13.3. Physical Security and Operational Lessons: The Case of Puma Shen

The threat posed by Chinese intelligence and security services has long since moved beyond the realm of cognitive manipulation and manifests itself in physical violence. The case study of renowned

DPP politician and leading candidate for the office of Taipei Mayor **Puma Shen** (沈伯洋) illustrates this escalation.¹¹⁰ Shen, a prominent expert on cognitive warfare, is not only exposed to physical attacks in parliament by forces that effectively act as an extension of Beijing, but has also become the target of a highly complex assassination plot. The fact that the *National Security Bureau (NSB)* was only able to intervene at the last second, when a supposed specialist in protective equipment—in reality an agent of Chinese state security—gained direct access to Shen's private quarters, reveals glaring gaps in security screening.

This incident must serve as a wake-up call for a radical reform of personal security and the vetting process. There is a need for a thorough clearance of all service providers and individuals who have access to decision-makers. The ease with which agents can infiltrate under the guise of "specialists" is evidence of a dangerous operational naivety that can be fatal in an environment of widespread infiltration.

13.4. Society-wide Defense and Asymmetric Resilience

Military deterrence against the PRC remains indispensable, but it is incomplete without societal resilience. The presence of over 1,000 U.S. military advisors is an important signal of support, but it must not lead to strategic passivity. **Taiwan's civil society should prepare for the scenario of a protracted asymmetric conflict.**

The population must **be comprehensively prepared for the reality of guerrilla warfare 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. At the same time, the financial flows of religious organizations, elected officials, and Taiwanese businesspeople from the PRC must be monitored without exception. Vigilance against infiltration attempts must also be enshrined as a national civic duty. Only a society that is prepared to actively defend every inch of ground and every institution will make the costs of aggression incalculable for Beijing.

13.5. The Cognitive Firewall: Education and Media as Defensive Weapons

The fight against infiltration begins in the minds of the people. Attempts at infiltration fail where an informed public pits historical truth against ideological manipulation. **The education system must therefore be understood as a strategic defensive weapon. It is essential to embed the history of the Chinese Communist Party in its full, unvarnished brutality into the curriculum.**

Schoolchildren and students must be better informed about the crimes of the regime in mainland China—from the Great Leap Forward and the Cultural Revolution through the Tiananmen Square massacre to the current oppression in Tibet,

Xinjiang, and Hong Kong. Only those who understand the nature of totalitarian rule in Beijing are immune to the promises of United Front propaganda. **Furthermore, civil resistance and crisis management should become part of school education** to strengthen societal self-organization under pressure.

At the same time, the media landscape must undergo a 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.

Democracy is all too often misunderstood in Taiwan as freedom without limits. **Analogous to the ban on Nazi propaganda, re-engagement in Nazi activities, and Holocaust denial in Germany and Austria, the legislative package regarding the promotion of the CCP or incitement to wage a war of aggression against Taiwan should finally be passed by the Legislative Yuan.**

The relationship between Germany and Austria, clouded by the crimes of the Third Reich, is often humorously described as follows: **“What divides us is our common language.”** This is even more true for Taiwan and China. **The bond of belonging to the Sino-Confucian cultural sphere is torn apart by vastly divergent social concepts—here a vibrant democracy, there the constitutionally enshrined “dictatorship of the proletariat.”**

The shared language opens the floodgates to media manipulation and misinformation. Children and young people in particular must be protected from this. **A ban on TikTok, which originated in China, and other highly manipulative, even toxic social networks—similar to the ban in Australia—would be extremely helpful in curbing Beijing’s cognitive warfare.**

13.6. Parliamentary Integrity and the “Fifth Column”

Taiwan has one of the most vibrant democracies in Asia. This political vitality is a strength—but it can become a weakness if parliamentary procedures are deliberately sabotaged.

Parliaments must not be a circus. The Legislative Yuan must be restored as a place of national dignity and sovereignty. The transformation of parliament into a venue for populist show fights and physical violence plays directly into the PRC’s narrative of discrediting democracy as a chaotic and doomed model.

Actors within **political parties such as the KMT or TPP, whose actions systematically advance Beijing’s strategic interests, must undergo a thorough security screening.** In cases of proven collaboration or funding by United Front bodies, the loss of parliamentary seats, the revocation of immunity, and criminal prosecution should be possible. Anyone who blocks parliamentary work through deliberate obstruction on behalf of a hostile power has no place in the people’s representative body.

Travel by elected officials to China must be prohibited until Beijing has signed a non-aggression pact with the ROC. In light of the espionage war that China is waging against Taiwan at all levels, this should also apply to representatives of municipal councils and local authorities.

13.7. 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. Therefore, European services should adopt the following:

1. **Strategic Exchange:** Cooperation with agencies such as the foreign intelligence service of the Federal Republic of Germany (BND), the German Federal Office for the Protection of the Constitution (BfV), the Federal Criminal Police Office (BKA), the CIA, and the British MI6, etc., should be massively intensified. 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. **Why, moreover, do European agencies not utilize Taiwanese experts to penetrate hostile Chinese networks within their own countries?**

2. **Canary Monitoring:** European states should use the infiltration patterns in Taiwan 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 the operations in Taipei.**

13.8. The Post-Xi Jinping Era. Diplomatic Creativity Versus Confrontation.

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. **In the long term, a political vision should be developed that offers a democratic alternative to authoritarian narratives.** The “one country, two systems” model has proven unworkable. What befell Hong Kong in 1997 after its “return to the motherland” was nothing but a loss of freedom. Even less does the autonomous status of Tibet, Xinjiang, or Inner Mongolia in a communist People’s Republic serve as an attractive promise of a future for the 23.5 million Taiwanese, who are accustomed to democracy.

But Germany and Austria could serve as a model. Why can’t two states with the same language and culture, despite an eventful and at times painful history, live peacefully side by side as close relatives, yet in separate homes? In civilized societies,

one does not immediately threaten one’s cousin with death and destruction simply because he has moved two houses down.

Another conceivable model would be a loose, confederal arrangement within a community of Chinese states. **Taiwan could make the signing of a peace or non-aggression pact with the PRC a precondition for resuming bilateral talks—backed by a binding mutual defense pact from Washington and democratic Asian neighboring states.** No one benefits from the disruption or even the destruction of Taiwan’s microchip manufacturing sites. And let us not forget that the PRC has always maintained full diplomatic relations with both German states, even though Beijing consistently asserts the One-China principle for itself.

De-escalation through the internationalization of the conflict could also be a further step. For example, through talks at the UN headquarters in Vienna under international observation. **The admission of Taiwan into the UN or other international organizations as “Taiwan,” following the model of the Soviet Union, could serve as a precedent. Although the USSR had “only” one vote on the UN Security Council, Ukraine and Belarus were each represented by their own seat in the UN General Assembly.**

Such considerations may seem utopian today, but they offer a strategic perspective that points beyond the mere status quo. They signal to the international com-

munity that Taiwan is not seeking confrontation, but rather a stable order based on freedom and democratic self-determination. Xi Jinping may now appear like an all-powerful emperor on the Dragon Throne, but even in Moscow and Beijing, history has at times turned virtually overnight. And Taiwan's government would be well advised to have plans in the drawer that extend beyond a single legislative term and have lasting social relevance.

13.9. Final Assessment

Taiwan's defense hinges on its ability to identify internal enemies and strengthen national resilience. Only a resilient democracy that is 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.**

Acknowledgments

This study was produced as part of the **Taiwan Fellowship 2025**. I would like to express my special thanks to the **Ministry of Foreign Affairs of the Republic of China (Taiwan)** for its generous support and for making this research visit possible, which formed the basis for the present analyses. I would also like to thank the extremely kind and helpful team at the Taiwan Fellowship office in the Central Library.

I would like to extend my special thanks to my host institution, **Soochow University** (東吳大學). I am deeply grateful to the **German Department** and the **Institute for Human Rights** (人權研究所) for allowing me to conduct research at this renowned institution. I would also like to personally thank my esteemed colleague **Dr. Jörg Parchwitz** for the valuable professional exchange and collegial support during my time in Taipei.

Without Professor Liu Wen-ping, the leading expert on cognitive warfare and united front issues, this work would hardly have been possible. His daily feedback was invaluable. I deeply appreciate that a friendship developed over more than a year of reading, learning, and researching. The same goes for Professor Kerry Gershaneck, whom I was always free to bother whenever I was stuck with technical questions, especially regarding the military aspects of my research.

I would like to extend special thanks to **Dr. Volker Stanzel**, my good friend and spiritual mentor. The opportunity to continuously exchange ideas with him has significantly shaped this work. It was an honor to accompany him on visits to Taiwanese government agencies and universities and to present there together with him. As a former Political Director at the Federal Foreign Office of the Federal Republic of Germany and Ambassador to Beijing and Tokyo, there was no better door-opener. I would also like to thank **Dr. Angela Stanzel**, Senior Associate, Asia Division, German Institute for International and Security Affairs (SWP), for her kind recommendation, which made this fellowship possible in the first place.

I would also like to extend special thanks to **Dr. Yu-cheng Chen** (陳育正), Associate Professor at the Graduate Institute of China Military Affairs Studies at the **National Defense University** (國防大學) in Taipei, particularly the **Chair of Cognitive Warfare**. It was a great honor to present and discuss my initial research findings in this expert forum. And I would also like to thank Vice **Minister Shen Yu-Chung of the Mainland Affairs Council (MAC)** for taking the time to explain the complex situation to me in detail.

Furthermore, I would like to thank the representatives of the Taiwanese security agencies, in particular the **Ministry of Justice Investigation Bureau (MJIB)**, experts associated with the **National Security Bureau (NSB)**, and the military counterintelligence service for their professional expertise. And a staff member associated with President Lai Ching-te. Thanks also to my colleagues at the **Institute for National Defense and Security Research (INDSR, 國防安全研究院)** and the **Prospect Foundation (遠景基金)**, the two leading think tanks in Taipei specializing in my research topic.

Special thanks go to the diplomatic representatives for their support: Taiwan's former Ambassador to Germany, **Prof. Dr. Shie Jhy-wey (謝志偉)**, as well as the Ambassador in Vienna, **Prof. Hans Suran-Yung Liu (劉玄詠)**, and their respective teams in Germany and Austria. Their outstanding commitment to bilateral exchange forms the backbone of projects of this kind.

The same applies to my many **friends in journalism and the media in Taiwan**, above all **Antonio Chiang (江春男)**, who continually inspire me through their commitment to press freedom. I would also like to thank **Dieter Schnaas**, the extremely astute and amiable copy-editor-in-chief of WirtschaftsWoche, who encouraged me to return to journalism with this project after a long hiatus.

Finally, it should be noted that the views, interpretations, and conclusions expressed in this study are the sole responsibility of the author and do not necessarily reflect the positions of the funding institutions, the security authorities, or the universities mentioned.

Note: This work was originally written in German, the author's native language. It was translated into English using the translation software deepL.com. As a result, there may be discrepancies in the use of Chinese or English technical terms.

Glossary

Table 1–1:

English (Sorting)	German	Chinese	Description / Function
1992 Consensus	1992-Konsens	九二共識	Political formula regarding “One China” that the PRC demands as the basis for talks.
AAAB Model	AAAB-Modell	AAAB模型	Stages of influence: Abroad, Adversaries, Attack, Benefits.
Active Measures	Aktive Maßnahmen	積極措施	Disinformation, sabotage, and influence operations aimed at destabilizing the adversary.
Anti-Infiltration Act	Anti-Infiltrationsgesetz	反滲透法	Taiwanese law designed to prevent political influence by the PRC.
APT41 (Barium)	APT41	APT41 / 雙龍	High-caliber Chinese hacking group; specializes in espionage and supply chain attacks.
ARATS	Vereinigung für die Beziehungen über die Taiwanstraße	海協會	Association for Relations Across the Taiwan Strait (PRC counterpart to the SEF).
Base 311	Basis 311	三一一基地	PLA Center for the “Three Wars” (psychological, media, and legal warfare) in Fuzhou.
BlackTech	BlackTech	黑客技術	Chinese APT group that primarily targets Taiwan and Japan (technology/government).
Central Military Commission (CMC)	Zentrale Militär-kommission	中央軍事委員會	Highest military leadership body of the CCP under Xi Jinping.

English (Sorting)	German	Chinese	Description / Function
Cognitive Warfare	Kognitive Kriegsführung	認知戰	Manipulation of thought through cyber operations and psychological subversion.
Comprehensive National Security Concept	Gesamtheitliches Sicherheitskonzept	總體國家安全觀	Xi Jinping's doctrine, which integrates security in the economic, ideological, and technological spheres.
Counter-Espionage Law	Spionageabwehrgesetz	反間諜法	Law of the PRC for the legal prosecution of "suspicious" foreign activities.
Critical Infrastructure	Kritische Infrastruktur	關鍵基礎設施	Sectors such as energy and water; the main target of Volt Typhoon.
Cyber Espionage	Cyberspionage	網絡間諜	Theft of data and intellectual property by state-sponsored hacking units.
Deepfake	Deepfake	深度偽造	AI-generated audio or video manipulation intended to deceive the public.
Dual-use technology	Güter mit doppeltem Verwendungszweck	雙重用途技術	Civilian technologies that can be used for military purposes (a target of Chinese acquisition).
Economic Coercion	Wirtschaftlicher Zwang	經濟脅迫	Use of trade embargoes or boycotts for political blackmail.
FIMI	Informationsmanipulation	外國資訊操弄與干擾	Foreign Information Manipulation and Interference (EU term for interference).
Gray Zone Operations	Grauzonen-Operationen	灰色地帶行動	Military and civilian pressure just below the threshold of open war.
Humint	Menschliche Aufklärung	人力情報	Traditional espionage conducted by agents and informants on the ground.

English (Sorting)	German	Chinese	Description / Function
Hybrid Warfare	Hybride Kriegsführung	混合戰	A combination of military, digital, and economic means of combat.
Information Support Force (ISF)	Informationsunterstützungstruppe	信息支援部隊	A branch of the PLA newly established in April 2024 for networked warfare.
Lawfare / Legal Warfare	Rechtliche Kriegsführung	法律戰	Use of laws (e.g., Anti-Secession Law) to legitimize violence.
MAC	Rat für Festlandsangelegenheiten	陸委會	Mainland Affairs Council: Taiwanese government agency responsible for China policy.
Ministry of Public Security (MPS)	Ministerium für öffentliche Sicherheit	公安部	PRC Ministry of Public Security; responsible for domestic intelligence and social control.
Ministry of State Security (MSS)	Ministerium für Staatssicherheit	國家安全部	China's primary foreign intelligence service (similar to the CIA/BND).
MJIB	Investigativ-Büro (Taiwan)	法務部調查局	Taiwanese counterintelligence agency under the Ministry of Justice.
National Intelligence Law	Nationales Geheimdienstgesetz	國家情報法	Law (2017) that can compel Chinese citizens to cooperate in espionage. Implementation is controversial.
NSB	Nationales Sicherheitsbüro (Taiwan)	國家安全局	Taiwan's central intelligence agency for foreign intelligence.
NSC	Nationaler Sicherheitsrat (Taiwan)	國家安全會議	Strategic advisory body to the Taiwanese president.
PLA	Volksbefreiungsarmee	人民解放軍	The armed forces of the People's Republic of China (under the command of the CCP).

English (Sorting)	German	Chinese	Description / Function
Psychological Warfare	Psychologische Kriegsführung	心理戰	A strategy to undermine the fighting spirit and morale of the population.
Public Opinion Warfare	Medienkrieg-führung	輿論戰	The battle for dominance in public opinion on social media and in the press.
Red Brigade	Rote Brigade	紅隊	Historical predecessor of the MSS (Zhongyang Teke); responsible for assassinations.
Salami slicing	Salami-Taktik	割肉戰術	A method of permanently shifting the status quo through many small steps.
SEF	Stiftung für Austausch (Taiwan)	海基會	Straits Exchange Foundation: Taiwan's semi-official negotiating body.
Sharp Power	Sharp Power	銳實力	The manipulative exercise of power through censorship and disinformation abroad.
Strategic Support Force (SSF)	Strategische Unterstützungstruppe	戰略支援部隊	Former PLA unit for cyber, space, and electronic warfare.
Supply Chain Attack	Lieferketten-Angriff	供應鏈攻擊	Infiltration of malware via legitimate updates (a specialty of APT41).
TAO	Büro für Taiwan-Angelegenheiten	國台辦	PRC government agency responsible for operational Taiwan policy.
Teke	Spezialabteilung der KPCh	特科	Abbreviation for Zhongyang Teke; the CCP's first intelligence apparatus.
Three Warfares	Drei Kriegsführungen	三戰	PLA doctrine: psychological, media, and legal warfare.
Transnational Repression	Transnationale Repression	跨國鎮壓	Global surveillance and intimidation of Chinese dissidents.

English (Sorting)	German	Chinese	Description / Function
UFWD	Arbeitsabteilung Einheitsfront	統一戰線	Office of the CCP Central Committee for influencing non-communist groups.
United Front	Einheitsfront	統一戰線	Network for co-opting elites and neutralizing enemies.
Volt Typhoon	Volt Typhoon	伏特颱風	PRC hacker collective dedicated to sabotaging critical U.S. infrastructure.
Wolf Warrior Diplomacy	Wolfskrieger-Diplomatie	戰狼外交	Aggressive diplomatic style of the PRC to defend national interests.

Current Overview of Leadership Roles in the PRC’s Intelligence and Security Services (as of March 2026)

Table II–1: Chronology of Ministers of State Security (MSS)

Name	Chinese	Term of office
Ling Yun	凌雲	1983–1985
Jia Chunwang	賈春旺	1985–1998
Xu Yongyue	許永躍	1998–2007
Geng Huichang	耿惠昌	2007–2016
Chen Wenqing	陳文清	2016–2022
Chen Yixin	陳一新	since 2022

Source: Mattis, P. / Brazil, M. (2019): *Chinese Communist Espionage*. Supplemented by current appointment decrees of the National People’s Congress through 2026.^[1]

Table II–2: Current Vice Ministers of the MSS (as of 2026)

Name	Chinese	Function
Yuan Yikun	袁亦鯤	US Analysis (formerly Yuan Peng)
Shi Haoyong	石浩勇	Operations Management
Tang Dai	唐岱	Administration & Planning
Nie Furu	聶福如	Political Discipline (Former MPS)

Source: Joske, A. (2022/2025): *Spies and Lies*. Updated by China Leadership Monitor 2026.^[2]

Table II–3: Leadership Roles in the Intelligence Community

Institution	Function	Name	Chinese
MSS	Minister	Chen Yixin	陳一新
MPS	Minister	Wang Xiaohong	王小洪
ISF	Commander	Bi Yi	畢毅
UFWD	Director	Li Ganjie	李幹傑

Source: IISS Military Balance 2025/2026. The SSF was reorganized into the Information Support Force (ISF) in April 2024. ^[3]

Table II–4: The New Structure of Military Intelligence (as of 2026)

New Unit	Chinese	Core Mission	Significance for the IC
ISF (Information Support Force)	信息支援部隊	Coordination of information systems	Central hub for data flows
Cyberspace Force	網絡空間部隊	Cyber Warfare & SIGINT Operations	Key player in cyber espionage
Aerospace Force	軍事航天部隊	Space Reconnaissance (IMINT)	Strategic Long-Range Reconnaissance

Source: IISS Military Balance 2026 & Ministry of National Defense Briefing. ^[4]

Table II–5: Command Structure of the Military Intelligence Branches

Function / Unit	Name	Chinese
Commander of the ISF	Bi Yi	畢毅
Political Commissar, ISF	Li Wei	李偉
Head of Cyberspace Force	Classified	—

Source: China Leadership Monitor (Spring 2026) & Saunders, P. C. et al. (2025). ^[5]

Bibliography for Table I-1 to II-5:

- [1] Mattis, P. / Brazil, M. (2019/2024): Chinese Communist Espionage. Naval Institute Press.
- [2] Joske, A. (2022): Spies and Lies. Hardie Grant.
- [3] IISS: The Military Balance 2026. Oxford University Press.
- [4] CSIS (2026): Mapping China’s Intelligence Infrastructure.
- [5] Saunders, P. C. et al. (2025): The PLA Beyond the 20th Party Congress. NDU Press.

Footnotes and Notes on the Text

Chapter 1 – Introduction: Why Focus on Chinese Espionage? The Battlefield of Perception – China’s Strategy Toward Taiwan in Light of Geopolitical and Psychological Paradoxes.

- 1 Kremb, Jürgen/ Von Wedel, Michael: The Reckoning: A Former BKA Agent Spills the Beans. Munich 2008.
- 2 Video: Mike Chinoy on Assignment China: An Oral History of American Journalists in the People’s Republic. USC US-China Institute. April 13, 2023. Accessed on: December 31, 2025 Available at: <https://china.usc.edu/node/19835>
- 3 Kremb, Jürgen: Until the Last Breath. Wei Jingsheng and the Fate of a Chinese Family, Munich 1997.
- 4 Kremb, Jürgen: “Shut Up, This Is China,” in DER SPIEGEL, 48/1998, November 22, 1998.
- 5 Chern, Chen: 中央研究眼, 週報第1566期/ “The Intelligence Connection be-tween West Germany and Taiwan. An Unknown Chapter of the Cold War,” December 6, 2025. Available at: <https://newsletter.sinica.edu.tw>
- 6 Background briefing
- 7 Background briefing
- 8 Focus Taiwan: Taiwan urges China not to attach political conditions to cross-strait travel. December 18, 2024. Available at: <https://focustaiwan.tw>
- 9 Taipei Times: Research Center Set Up to Combat Cognitive Warfare, January 19, 2024, Available at: www.taipei-times.com.
- 10 Background Briefing

Chapter 2 – In the Eye of the Storm – The Academic Debate on Cognitive Warfare and Hybrid Threats

- 11 Liu, Wen-ping: New Awareness of Cognitive Warfare (Taipei: Independent Author, 2025), p. 22.
- 12 Liu, Wen-ping: "Research on Negative Effects and Responses to Cognitive Warfare – Communication Obstacles and Interpretation," Nanhua Social Science Forum (Chiayi), Vol. 16, July 2024, p. 70.
- 13 "The Origin of the Concept of the United Front," United Front Work Department of Luoyang Normal University, accessed August 22, 2018, Available at: <https://sites.lynu.edu.cn>.
- 14 Yang, Tai-yuan: "The Meaning and Development Trend of the PLA's 'Gray Zone Harassment' in the Waters Around Taiwan" (May 28, 2024), accessed November 15, 2025, China Studies Institute, Available at: <https://iccs.org.tw>.
- 15 "Chinese Coast Guard Dark Ships Continue Harassment, Invading Kinmen Waters Again Today" (November 11, 2025), accessed November 13, 2025, Coast Guard Administration, Ocean Affairs Council, Available at: www.cga.gov.tw.
- 16 Chen Yu-sheng, Zhong Zhang-han: "Apocalypse of the Ukraine War: The Whole Network Responds, Guarding the Discourse Power of War! How Can Taiwan Win the 'Hybrid War'?" (March 7, 2022), accessed November 13, 2025, Commonwealth Magazine, Available at: www.cw.com.tw.
- 17 Gershaneck, Kerry: Political Warfare: Strategies for Combating China's Plan to 'Win Without Fighting', Marine Corps University Press, 2020.

Chapter 3 – The Architecture of the "Secret Front" – The Genesis of Chinese Intelligence Services Regarding the KMT and Taiwan

- 18 Weng, Yanqing: Taipei. 2022. The Communist Party of China Intelligence Organization & Spy. pp. 2–3. (翁衍慶: 中共情報組織與間諜活動.)
- 19 See also: Weng, Yanqing.
- 20 Ibid., pp. 5–7 (case studies on the infiltration of the Nationalist Army).
- 21 Weng, Yanqing: Taipei. 2022. The Communist Party of China Intelligence Organization & Spy. p. 15 ff. (Weng Yanqing: The Communist Party of China Intelligence Organization & Spy.)
- 22 For legal developments and their impact on Taiwan, see Chapter IV-7a)

- 23** See Footnote 21.
- 24** See Footnote 21.
- 25** Intelligence Service Report: The Ministry of State Security's Operations
- 26** CSIS: Survey of Chinese Espionage in the United States since 2000
- in the Taiwan Strait, in: Journal of Strategic Intelligence, Vol. 14, No. 2, 2024, p. 88

Chapter 4 – The Power of sheer numbers. Personnel and structures

- 27** Alex Joske, Spies and Lies: How China's Greatest Covert Operations Fooled the World, Hardie Grant Books, 2022, pp. 45–52.
- 28** Estimates based on IISS (2025): The Military Balance 2025 and DOD (2025): China Military Power Report.
- 29** Peter Mattis / Matthew Brazil, Chinese Communist Espionage: An Intelligence Primer, Naval Institute Press, 2019, pp. 31–40.
- 30** Alex Joske & YunGeun Jeon, 'Re-designing state security: The 2018 reorganisation of the Ministry of State Security', Deserepi 1, 2025, pp. 16–17.
- 31** Ibid.
- 32** Doublethink Lab (2026): China's AI-Driven Influence Operations in the 2025 Election Cycle.
- 33** Cf. Liu Te-liang: Training material for Taiwanese recruits.
- 34** Intelligence Service Report: The Ministry of State Security's Operations in the Taiwan Strait, in: Journal of Strategic Intelligence, Vol. 14, No. 2, 2024, p. 88.
- 35** Clive Hamilton / Mareike Ohlberg: The Silent Conquest: How China Is Undermining Western Democracies, 2nd ed., DVA, 2023, p. 112.
- 36** Anne-Marie Brady: Magic Weapons: China's Political Influence Activities under Xi Jinping, ASPI, 2017; Center for Strategic and International Studies (CSIS), Survey of Chinese Espionage, and Nicholas Eftimiades, Chinese Intelligence Operations, Naval Institute Press, 1994.

Chapter 5 – Shadows on the Net. The Role of Advanced Persistent Threats (APTs)

- 37** IISS (2025): The Military Balance 2025: China's New Information Support Force (Xīnxī Zhīyuán Bùduì), pp. 238–242.
- 38** Microsoft Threat Intelligence (2025): Volt Typhoon targets US critical infrastructure with living-off-the-land techniques, March 2025 update.
- 39** Kendzierskyj, Stefan; Jahankhani, Hamid, *Critical National Infrastructure, C4ISR and Cyber Weapons in the Digital Age*, Advanced Sciences and Technologies for Security Applications, Cham: Springer International Publishing: 3–21.
- 40** Mandiant (Google Cloud) (2025): APT41: World War C - The Evolution of a Chinese State-Sponsored Group, Special Report, pp. 14–19.
- 41** Recorded Future (Insikt Group) (2025): RedJuliett: Targeted Intelligence Collection Operations Against Taiwan, Research Report June 2025.

Chapter 6 – The Facets of the CCP's Cognitive Warfare in Democratic Countries, Including Taiwan.

- 42** The information in Chapter 6 is derived primarily from interviews and background discussions with security services and is cited here as background discussion. (See also: General Information: Author interview confidential, 2025). See: 展望與探索雜誌社. The Prospect & Exploration Magazine Society. Taipei, Taiwan, May 2025.

Chapter 7 – Analysis of Chinese Espionage Activities. Have 5,000 or even 100,000 Chinese agents infiltrated Taiwan?

- 43** Liu, Te-liang (2025): A Brief Discussion on the State of Communist Espionage in Taiwan, in: Cross-Strait Situation Analysis Bulletin (DPP), August 2025.
- 44** Ibid.
- 45** China's infiltration of Taiwan is serious, Liberty Times Net (LTN), August 16, 2025.
- 46** Quoted from Liu, Te-liang (2025): National Security Intelligence Practice Research, Training Material (PP presentation), slide "In 2007."
- 47** See Liberty Times Net (2025).
- 48** See Liu, Te-liang (2025), Training Materials, slide "News Formats".

- 49** See Han, Kun (2000), cited in Liu, Te-liang (2025), training materials, slide “In 2000”.
- 50** See Liu, Te-liang: 2025, training materials, slide: “Eighteen years later”.
- 51** Data from the National Security Bureau (NSB): cited in Liu, Te-liang (2025), training materials.
- 52** See Liu, Te-liang: Training materials, slide “The Democratic Progressive Party (DPP) recently exposed four spies”.
- 53** See Liu, Te-liang: Training materials, slide: “Cultivate sound life habits.”
- 54** National Security Bureau (NSB): Analysis of China’s Cognitive Warfare Tactics Against Taiwan in 2025, January 11, 2026, p. 1.
- 55** Ibid.
- 56** See NSB Report (2026): p. 1, section on “narrative themes and tones”.
- 57** Ibid., section “using data to analyze Taiwan’s social dynamics.”
- 58** Ibid., p. 1.
- 59** Ibid.
- 60** Ibid.
- 61** Ibid., concluding section on the implementation of reporting mechanisms.
- 62** Ibid., section on international cooperation (security dialogues).
- 63** Cf. Liu, Te-liang: (2025), Training Materials, slide “The chapter on espionage in Sun Tzu’s Art of War.”

Chapter 8 – Religious Infiltration and the “Iron Triangle” – The Instrumentalization of Mazu Worship and Organized Crime

- 64** Mazu, Political Influence and Organized Crime in Taiwan, Papers on contemporary religion, Religioscope Institute, April 2025, p. 4 ff.
- 65** Ibid., Chapter 03: “The Iron Triangle: Taiwanese Gangs, Mazu Temples, and the CCP,” p. 21.
- 66** See ibid., Chapter 06: “The Bamboo Union and Cross-Strait Influence,” p. 43.
- 67** See ibid., Chapter 04: “The Dajia Jenn Lann Temple,” p. 29.
- 68** See ibid., Chapter 05: “The Taiwan Mazu Fellowship Association,” p. 37.
- 69** See ibid., p. 24 ff. (section on criminal financing).
- 70** See ibid., Chapter 07: “The Tianjin Binhai Mazu Cultural Park,” p. 49.

71 See *ibid.*, Concluding Remarks, p. 56.

72 See *ibid.*, p. 45 (analysis of criminal militias).

73 Daly, Mattias Swenson: Infiltrating the Tao. United Front Influence Operations Targeting Quanzhen Taoist Communities in Taiwan and the West. Religioscope 2025. Fribourg, Switzerland.

Chapter 9 – The Political Turn of 2025 – President Lai’s Security Agenda and the New Wave of Legislation

74 The exact text of President Lai’s speech can be found here: www.president.gov.tw. “President Lai holds press conference following high-level

national security meeting.” Office of the President, Republic of China (Taiwan). Accessed March 13, 2025.

Chapter 10 – Strategic Paralysis – The “Fifth Column” and the Erosion of Parliamentary Stability

75 Chinese spouse faces scrutiny before joining Taiwan legislature, Taiwan News, November 8, 2024. And: KMT Chair Eric Chu to skip security briefing, Taiwan News, June 17, 2025.

76 TPP defense budget sent to review, Cabinet version blocked, Taipei Times, January 30, 2026.

77 *Ibid.* See also statement by Government Spokesperson Michelle Lee (李慧芝).

78 Taiwan News: Chinese spouse faces scrutiny before joining Taiwan legislature, Taiwan News, November 8, 2024.

79 *Ibid.*

80 Jamestown Foundation: China’s United Front Work in Taiwan: A 2025 Assessment, Washington, D.C., 2025, pp. 12–18.

81 *Ibid.*

82 Kremb, Jürgen: Essay, Taiwan – China’s War Against the Country Has Long Since Begun. WirtschaftsWoche, February 25, 2026.

Chapter 11 – The “Japan Crisis” – Geopolitical Escalation and Cognitive Synchronization

- 83** IORG Weekly Report No. 128: The CCP’s Complex Threats Against Japan, December 29, 2025, p. 1.
- 84** Ibid. (reference to Xue Jian).
- 85** See Taiwan Information Environment Research Center (IORG): E-Newsletter December 2025, published on December 29, 2025.
- 86** People’s Daily (人民日報): Commentary “Zhongsheng” (鐘聲), November 14, 2025.
- 87** See IORG Report 128, section “Measures to Exert Pressure.”
- 88** Ibid. (Reference to the pandas at Ueno Zoo).
- 89** See IORG Analysis: Discourse on Japan and the Coordination Between the CCP, KMT, and TPP, December 2025.
- 90** Ibid. (Use of the terms “militarism” and “aggressor”).
- 91** See IORG Monthly Report, December 2025, section “Division of Labor in U.S. Discourse.”
- 92** IORG Newsletter No. 128: Statements by Ma Ying-jeou, Hung Hsiu-chu, and Kao Chin-su-mei.
- 93** See IORG analysis on the defamation of President Lai and the statements by Su Ching-chuan.
- 94** See IORG Final Report 2025: Threats from Authoritarian Regimes and Information Manipulation.

Chapter 12 – Specific Espionage Cases and Criminal Consequences

- 95** Reuters: Taiwan reports ‘significant rise’ in suspected Chinese espionage. January 13, 2025. www.reuters.com
- 96** Central News Agency (CNA): “Chairman of the Rehabilitation Alliance Party sentenced to 10 years in prison,” Jan. 29, 2026.
- 97** Focus Taiwan (CNA English): “Former Presidential Guards Sentenced for Military Espionage,” March 10 / Dec. 5, 2025.
- 98** CNA/ Central News Agency: “Former Pilot Sentenced to 2 Years and 2 Months for Recruiting Military Officers to Leak Training Secrets to China.” Aug. 21, 2025. 11:23 a.m.

- 99** AP News / CNA: “Four former DPP staff sentenced for spying,” Sept. 25, 2025.
- 100** Taipei Times: Diabolo instructor and his spy ring sentenced to jail. July 1, 2025.
- 101** Taipei Times: “CUPP members sentenced for National Security Act violations,” March 2025.
- 102** Taipei Times: “Prosecutors indict seven in military espionage ring,” Nov. 19, 2025.
- 103** AA. Taiwan confirms 2 air force officers indicted for espionage. Men allegedly supplied secret training documents containing sensitive information to China. Saadet Gokce. March 12, 2025.
- 104** Taiwan News: “Reserve captain indicted for selling secrets via Telegram,” Nov. 11, 2025.
- 105** AP News: “Journalist detained over alleged military bribery,” Jan. 8, 2026.
- 106** Taiwan News: Taiwan Cabinet greenlights amendments to National Security Act; amendments target people advocating war against Taiwan. December 18, 2025.
- 107** Classified National Security Information Protection Act (國家機密保護法), last amend-ed on Dec. 27, 2023, Laws & Regulations Database of The Republic of China (Taiwan), available at: <https://mojlaw.moj.gov.tw> (accessed on March 8, 2026).
- 108** Anti-Infiltration Act (反滲透法), promulgated on Jan. 15, 2020, Laws & Regulations Database of the Republic of China (Taiwan), available at: <https://law.moj.gov.tw> (accessed on Mar. 8, 2026).
- 109** Criminal Code of the Armed Forces (陸海空軍刑法), last amended on May 13, 2009 (or most recent version), Law and Regulation Database of the MND (Taiwan), available at: <https://law.mnd.gov.tw> (accessed on March 8, 2026).

Chapter 13- Strategic Recommendations: The Defensible Republic

- 110** Kremb, Jürgen: Essay. Chinas Krieg gegen Taiwan hat längst begonnen. (Engl: China’s War Against the Country Has Long Since Begun). WirtschaftsWoche, February 25, 2026

Bibliography and List of Sources

1. Books and Monographs (International Standard Works)

Allen, Bethany (2023): *Beijing Rules: How China Weaponized Its Economy to Confront the World*.

Bardenhagen, Klaus (2024): *The Most Important Island in the World: What Is at Stake in Taiwan*.

Brady, Anne-Marie (2017): *Magic Weapons: China's Political Influence Activities under Xi Jinping*. Canberra: ASPI.

Brazil, Matthew / Mattis, Peter (2019): *Chinese Communist Espionage: An Intelligence Primer*. Annapolis: Naval Institute Press.

Byron, John / Pack, Robert (1992): *The Claws of the Dragon: Kang Sheng – The Evil Genius Behind Chairman Mao*.

Cole, J. Michael (2017): *Taiwan's Security: History and Prospects*. London: Routledge.

Deacon, Richard (1974): *The Chinese Secret Service*.

Demes, David (2025/26): *Analyses of Taiwan's Political Landscape and Security*.

Easton, Ian (易思安) (2017): *The Chinese Invasion Threat: Taiwan's Defense and American Strategy in Asia*.

Eftimiades, Nicholas (2022): *Chinese Espionage: Operations and Tactics*. 2nd edition (Original 1994, Annapolis: Naval Institute Press).

Faligot, Roger (2019/2024): *Chinese Spies: From Chairman Mao to Xi Jinping* (German title: *Der Meister der Schatten*). London: Hurst.

Faligot, Roger (2022): *The Chinese Secret Service: From Mao to Now*.

Fulda, Andreas (2024): *Germany and China: How Entanglement Undermines Freedom, Prosperity, and Security*. London: Bloomsbury Academic.

Fulda, Andreas (2026): *When China Attacks: A Scenario*. Munich: C.H. Beck (Beck Paperback, Vol. 6629).

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

Gutmann, Ethan (2014): *The Slaughter (as well as works on the "War against America")*.

Hamilton, Clive / Ohlberg, Mareike (2020/2023): *Hidden Hand / The Silent Conquest: How the CCP Is Reshaping the World*. London: Oneworld / Munich: DVA.

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

Kremb, Jürgen and Wedel, Michael (2008): *The Reckoning. An Ex-BKA Agent Spills the Beans*. Munich: Herbig.

Kremb, Jürgen: *Until the Last Breath: Wei Jingsheng and the Fate of a Chinese Family*, Munich 1997.

Lowenthal, Mark M. / Clark, Robert M. (2024): *Chinese Intelligence Operations*. Washington, DC: Georgetown University Press.

Shambaugh, David (2008): *China's Communist Party: Atrophy and Adaptation*. Berkeley: University of California Press.

Shum, Desmond (2021): *Red Roulette: An Insider's Story of Wealth, Power, and Vengeance in Today's China*.

Weng, Yanqing (翁衍慶) (2022): *The Communist Party of China Intelligence Organization & Spy*. Taipei.

2. Academic Articles and Specialized Papers

Chen, Chern (2025): "The Intelligence Connection between West Germany and Taiwan. An Unknown Chapter of the Cold War." Academia Sinica Newsletter / Weekly.

Liu, Wen-ping (劉文斌) (2024): "Research on Negative Effects and Responses to Cognitive Warfare." Nanhua Social Science Forum.

Liu, Wen-ping (劉文斌) (2025): "New Awareness of Cognitive Warfare" as well as scholarly essays on the anatomy of cognitive warfare (MJIB).

Yang, Tai-yuan (2024): "The Meaning and Development Trend of PLA Gray Zone Operations." Institute of China Studies.

3. Reports from think tanks and research institutes

Australian Strategic Policy Institute (ASPI): *China's United Front and Influence Operations*.

Center for Strategic and International Studies (CSIS): *Survey of Chinese Espionage in the United States since 2000*.

Doublethink Lab (2026): *China's AI-Driven Influence Operations in the 2025 Election Cycle*.

International Institute for Strategic Studies (IISS) (2025): *The Military Balance 2025* (including analyses of the Information Support Force).

Jamestown Foundation: China Brief (Various issues on intelligence services and the PLA, including “*China’s United Front Work in Taiwan: A 2025 Assessment*”).

Prospect & Exploration Magazine Society (展望與探索雜誌社): *The Analysis on Chinese Influence and Intelligence Networks* (Taipei, May 2025).

RAND Corporation: *Chinese Influence Operations in the Indo-Pacific* (studies on salami tactics).

Religoscope Institute (2025): *Mazu, Political Influence, and Organized Crime in Taiwan*.

4. Government Reports and MJIB Publications

Ministry of Justice Investigation Bureau (MJIB) – *Prospect & Exploration* (展望與探索): Monthly journal on security issues, counterintelligence, and Mainland China studies.

Ministry of Justice (Taiwan): Anti-Espionage Laws and National Security Legislation.

National Security Bureau (NSB), Taiwan (2026): Analysis of China’s Cognitive Warfare Tactics Against Taiwan in 2025, as well as annual situation reports on the United Front.

National Security Council (NSC), Taipei (2025): *Analyses of cross-border influence operations*.

Taiwan Coast Guard Administration / Ocean Affairs Council (2026): Official Maritime Security Reports on incidents near Kinmen.

U.S. Department of Defense (2025): Annual Report to Congress: Military and Security Developments Involving the People’s Republic of China. Washington.

5. Newspaper Articles and Media Reports

CommonWealth Magazine (2022): “*Apocalypse of the Ukraine War: How Taiwan Can Win the Hybrid War*” (March 7, 2022).

Focus Taiwan (2024): “*Taiwan Urges China Not to Attach Political Strings to Cross-Strait Travel*” (December 18, 2024).

Kremb, Jürgen (2026): “*Chinas Angriff auf Taiwan hat längst begonnen/ Engl: China’s Attack on Taiwan Has Long Since Begun,*” *WirtschaftsWoche* (February 25, 2026).

Reuters (2025): “*Taiwan Reports Significant Rise in Suspected Chinese Espionage*” (January 13, 2025).

Taipei Times (2024): “*Research Center Set Up to Combat Cognitive Warfare*” (January 19, 2024).

Taipei Times (2026): “*Chinese Coast Guard Harassment near Kinmen Continues*” (January 30, 2026).

6. Online Sources and Digital Documents

Academia Sinica: Newsletter and archived publications on the history of intelligence services.

Buckley, Michael (2024): *“The End of China’s Rise and the Future of World Order”* (World Knowledge Forum) and *“China’s Turn to Fascist Rule”* (The Globalist).

Microsoft Threat Intelligence (2025): *“Volt Typhoon Targets Critical Infrastructure.”*

Mandiant / Google Cloud (2025): *“APT41: World War C – The Evolution of a Chinese State-Sponsored Group.”*

Recorded Future / Insikt Group (2025): *“RedJuliett: Targeted Intelligence Collection Operations Against Taiwan.”*

Index of Names

(Alphabetical by English Spelling)

Allen, Bethany – U.S. journalist and author; focuses on China's economic leverage.

Allen, Kenneth – U.S.-China military expert; former USAF intelligence officer.

Bardenhagen, Klaus – Journalist and author; focuses on Taiwan.

Brady, Anne-Marie – Political scientist; research on Chinese influence operations and the United Front.

Brazil, Matthew – China expert; former U.S. diplomat and co-author on Chinese espionage.

Buckley, Michael – Journalist and author focusing on political developments in China.

Bush, Richard C. – Brookings researcher on Taiwan-China relations.

Byron, John – Pseudonym of a diplomat and author on Kang Sheng.

Campbell, Kurt – U.S. diplomat; architect of the Indo-Pacific strategy.

Chen, Chen-yuan – 陳振遠 – Taiwanese security analyst.

Chen, Chern – 陳志宏 – Historian at Academia Sinica; expert on the history of intelligence services.

Chen, Ming-tong – 陳明通 – Former Director of the National Security Bureau (NSB) of Taiwan.

Chen, Yu-sheng – 陳昱勝 – Journalist and expert on hybrid warfare.

Cheng Li-wun – 鄭麗文 – Politician; Chairwoman of the Kuomintang (KMT).

Chiang, Antonio – 江春男 – Renowned journalist, columnist, and founder of the news magazine The Journalist (Xin Xinwen, 新新聞); former Deputy Secretary-General of Taiwan's National Security Council (NSC).

Clark, Robert M. – Expert in intelligence analysis.

Cole, J. Michael – Security analyst based in Taiwan.

Deacon, Richard – Historian and author on Chinese intelligence.

Demes, David – Journalist and security analyst in Taiwan.

Dong, Jingwei – 董經緯 – Vice Minister of State Security (MSS) of the PRC.

Doshi, Rush – U.S. strategic expert on China policy.

Easton, Ian – U.S. security expert; author on the threat to Taiwan.

Eftimiades, Nicholas – Former US intelligence officer; expert on Chinese espionage operations.

Faligot, Roger – French investigative journalist and author on Chinese intelligence services.

Finkelstein, David – China military researcher.

Fulda, Andreas – Political scientist; expert on German-Chinese relations and Taiwan.

Gershaneck, Kerry – U.S. military expert and professor; specialist in political warfare.

Glaser, Bonnie – Director of the Indo-Pacific Program at GMF; expert on Taiwan policy.

Grossman, Derek – Senior defense analyst focusing on the Indo-Pacific.

Gutmann, Ethan – Author and human rights activist.

Hamilton, Clive – Professor and researcher on CCP influence operations.

Han, Kuo-yu – 韓國瑜 – Speaker of the Taiwanese Parliament.

Hsiao, Bi-khim – 蕭美琴 – Taiwanese diplomat; acting vice president.

Joske, Alex – 周安瀾 – Analyst and author on the operations of the Ministry of State Security.

Kania, Elsa – Expert on Chinese military technology and AI.

Kremb, Jürgen – 周勁恆 – Journalist (including DER SPIEGEL, NZZ, Handelsblatt), sinologist, and author. Taiwan Fellow 2025.

Lai, Ching-te – 賴清德 – President of the Republic of China (Taiwan).

Lee, Chen-hsiu – 李貞秀 – Chinese-born politician of the TPP.

Lee, Hsi-min – 李喜明 – Former Taiwanese Chief of the General Staff; advocate of asymmetric warfare.

Lee, Teng-hui – 李登輝 – Former President of Taiwan (1988–2000); “Father of Democracy.”

Li, Keqiang – 李克強 – Former Premier of the PRC (2013–2023).

Li, Shangfu – 李尚福 – Former Minister of National Defense of the PRC.

Liu, Te-liang – 劉德良 – Former Director of Taiwan’s Military Intelligence Bureau (MIB).

Liu, Wen-ping – 劉文斌 – Professor and expert on cognitive warfare (formerly MJIB).

Lowenthal, Mark M. – Regular contributor to intelligence analyses.

Ma, Ying-jeou – 馬英九 – Former President of Taiwan (2008–2016).

Mao, Zedong – 毛澤東 – Historical leader of the CCP.

Mastro, Oriana – Stanford researcher on PLA strategies.

Mattis, Peter – Former CIA analyst; researcher on Chinese intelligence services.

Mulvenon, James – Expert on the PLA and cybersecurity.

Nathan, Andrew – Political scientist at Columbia University.

Ohlberg, Mareike – GMF expert on the CCP's global influence research.

Pillsbury, Michael – US-China strategy advisor.

Saunders, Phillip C. – Expert on Chinese military strategy (NDU).

Scobell, Andrew – Military researcher specializing in the PLA.

Segal, Adam – Cybersecurity expert at the Council on Foreign Relations.

Shambaugh, David – Professor of International Relations and China Policy.

Sheena Chestnut Greitens – Security expert on authoritarian regimes and China.

Shen, Puma – 沈伯洋 – Co-founder of the Kuma Academy; expert on cognitive warfare and disinformation.

Shum, Desmond – 沈棟 – Former insider and author of “Red Roulette.”

Swaine, Michael – Expert on Chinese security policy.

Tsai, Ing-wen – 蔡英文 – President of Taiwan (2016–2024).

Wang, Huning – 王滬寧 – Chief Ideologist and member of the Standing Committee of the CCP.

Wang, Yi – 王毅 – Foreign Minister of the PRC.

von Wedel, Michael – Former BKA officer and expert on security issues.

Wei, Jingsheng – 魏京生 – Well-known Chinese dissident.

Wu, Joseph – 吳釗燮 – Former Minister of Foreign Affairs of Taiwan; Secretary-General of the NSC.

Xi, Jinping – 習近平 – General Secretary of the CCP and President of the PRC.

Yang, Andrew N.D. – 楊念祖 – Former Taiwanese Minister of National Defense.

Yang, Tai-yuan – 楊泰源 – Taiwanese military analyst and PLA expert.

Zhao, Lijian – 趙立堅 – Former spokesperson for the Chinese Ministry of Foreign Affairs.

Zhong, Zhang-han – 鍾章翰 – Security journalist; focuses on military intelligence.

Zhu, Feng – 朱鋒 – Professor of International Studies at Nanjing University.

Zhou, Bo – 周波 – Retired PLA colonel and strategic analyst.

About the Author



Jürgen Kremb

is a German author, journalist, and political analyst specializing in East and Southeast Asia, human rights, and security issues. He studied East Asian Studies (Sinology, Japanese, and Tibetan Studies), Economics, and Journalism at Freie Universität Berlin and in Taiwan.

For more than two decades, he headed the foreign bureaus of the news magazine **DER SPIEGEL in Beijing, Singapore, and Vienna.** There, he reported on political, economic, and security developments in Asia. He also wrote for the *Neue Zürcher Zeitung*, the *Handelsblatt*, and other German-language media.

His biography of the Chinese dissident **Wei Jingsheng** became a bestseller on the Chinese black market and, along with allegations that he possessed and disseminated state secrets, contributed to his **expulsion from the country by Chinese authorities within 48 hours in November 1998.**

During his tenure in Southeast Asia, Kremb conducted research into Islamist terrorism. He also teamed up with a BKA investigator to author the first insider report on **Germany's Federal Criminal Police Office.**

In 2008, after months of research, he was able to uncover how former German **Under Secretary of Defense for Armaments, Holger Pfahls**, was able to go into hiding from German and international investigators with the help of contacts in intelligence circles in Asia.

Today, Kremb lives in Vienna and mostly in Taiwan. In 2025, he was awarded the **Taiwan Fellowship.** As a visiting scholar, he currently conducts research on Chinese intelligence services and influence operations at **the Human Rights Institute of Soochow University in Taipei** (東吳大學人權研究所).

