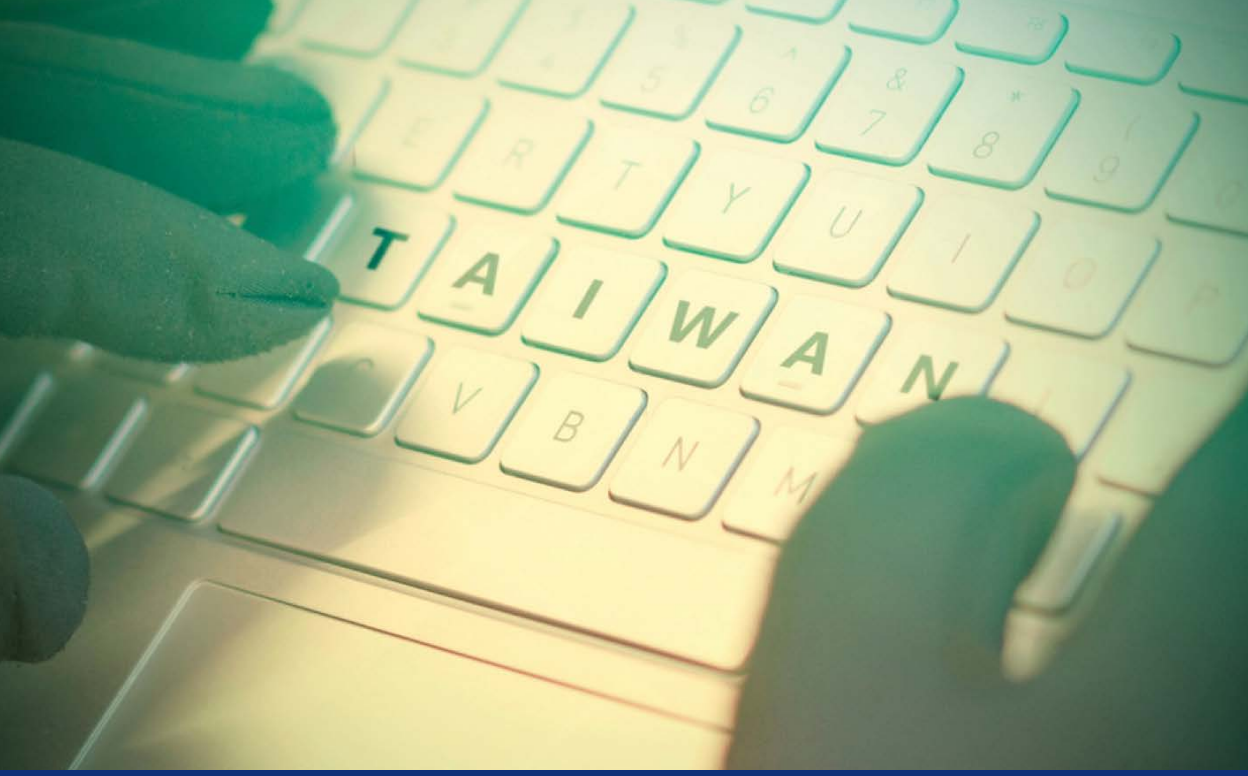


# Taiwan in the Hidden War

## The Contest for Technological Sovereignty Against Infiltration

Edited by

**Yi-Chieh Chen**

**Niklas Swanström**

Special Paper | March 2026

Institute for Security & Development Policy

# Taiwan in the Hidden War:

## The Contest for Technological Sovereignty Against Infiltration

Edited By

**Yi-Chieh Chen**

**Niklas Swanström**

Special Paper

March 2026

Institute for Security & Development Policy

"Taiwan in the Hidden War: The Contest for Technological Sovereignty Against Infiltration" is a Special Paper published by the Institute for Security and Development Policy. The Special Paper Series is the Occasional Paper series of the Institute's Asia Program, and addresses topical and timely subjects. The Institute is based in Stockholm, Sweden, and cooperates closely with research centers worldwide. The Institute serves a large and diverse community of analysts, scholars, policy-watchers, business leaders, and journalists. It is at the forefront of research on issues of conflict, security, and development. Through its applied research, publications, research cooperation, public lectures, and seminars, it functions as a focal point for academic, policy, and public discussion.



ISBN: 9978-91-88551-80-1

Distributed in Europe by:

Institute for Security and Development Policy
Västra Finnbodavägen 2, 131 30 Stockholm-Nacka, Sweden
Tel. +46-841056953; Fax. +46-86403370
Email: info@isdp.eu

Editorial correspondence should be directed to the address provided above (preferably by email).

Cover Photo: Znakki / Shutterstock

# Contents

# List of Abbreviations

| | |
|---|---|
| AI | Artificial intelligence |
| APT | Advanced Persistent Threat |
| ASPI | Australian Strategic Policy Institute |
| CAICT | China Academy of Information and Communications Technology |
| CCP | Chinese Communist Party |
| CISA | Cybersecurity & Infrastructure Security Agency |
| COSTIND | Commission for Science, Technology and Industry for National Defense |
| DPP | Democratic Progressive Party |
| DSET | Research Institute for Democracy, Society, and Emerging Technology |
| EU | European Union |
| FDPR | Foreign Direct Product Rule |
| IC | Integrated Circuit |
| IDM | Integrated Device Manufacturer |
| ITRI | Industrial Technology Research Institute |
| LLM | Large Language Model |
| MCF | Military-Civil Fusion |
| MIIT | Ministry of Industry and Information Technology |
| NATO | North Atlantic Treaty Organization |
| NSB | National Security Bureau |
| PLA | People's Liberation Army |
| PRC | People's Republic of China |
| PSMC | Powerchip Semiconductor Manufacturing Corporation |
| SOE | State-Owned Defense Enterprise |
| TSMC | Taiwan Semiconductor Manufacturing Company |
| U.S. | United States |
| UAV | Unmanned Aerial Vehicle |
| UMC | United Microelectronics Corporation |
| UUV | Unmanned Underwater Vehicles |
| VPN | Virtual Private Network |

# List of Contributors

**Niklas Swanström** is the Director of the Institute for Security and Development Policy, and one of its co-founders. He is a Fellow at the Foreign Policy Institute of the Paul H. Nitze School of Advanced International Studies (SAIS) and a Senior Associate Research Fellow at the Italian Institute for International Political Studies (ISPI). His main areas of expertise are conflict prevention, conflict management and regional cooperation; Chinese foreign policy and security in Northeast Asia; the Belt and Road Initiative, traditional and non-traditional security threats and its effect on regional and national security as well as negotiations. His focus is mainly on Northeast Asia, Central Asia and Southeast Asia.

**Yi-Chieh Chen** (陳奕傑) is a Project Manager and Research Fellow at the Institute for Security and Development Policy's Stockholm Taiwan Center (STC). She is also part of the Stockholm Center for Research and Innovation Security (SCRIS). She holds a Bachelor's degree in Arabic Language and Culture from National Chengchi University in Taiwan and a Master's degree in Global Studies from Gothenburg University in Sweden. Yi-Chieh Chen has a broad interest in East Asian affairs, soft power, and technology. Her research focus includes Taiwan-Europe relations, Cross-Strait relations, sports diplomacy, and the semiconductor industry.

**Yu-Chung Shen** (沈有忠) is currently the Deputy Minister of the Mainland Affairs Council of the Republic of China (Taiwan). He is also a Professor in the Department of Political Science at Tunghai University in Taichung, Taiwan. Dr. Shen received his Ph.D. from National Taiwan University in 2009. He has also served as a visiting scholar at the Free University of Berlin in Germany. His research interests include comparative politics, political institutions, and cross-strait relations between Taiwan and China. He has published articles in journals such as the Asian Journal of Political Science,

Taiwan Journal of Democracy, Journal of Power, Politics & Governance, Taiwanese Journal of Political Science, and Soochow Journal of Political Science, among others.

**Shiow-Wen Wang** (王綉雯) is an Assistant Research Fellow at the Institute for National Defense and Security Research (INDSR), where her research explores the strategic implications of U.S.-China technology competition, supply chain security, and innovation ecosystems. Wang's current work focuses on China's artificial intelligence development and the semiconductor-centered dynamics of this rivalry. Previously, Wang served as an Associate Research Fellow at the Taiwan Institute of Economic Research, conducting studies on European large-scale R&D initiatives and industry-academia-government collaboration mechanisms. At INDSR, she initially researched defense-industrial issues, with particular attention to U.S. and Japanese shipbuilding practices, before transitioning to the Division of Chinese Political and Military Affairs. She holds a Ph.D. in Law from Kyoto University.

**Yisuo Tzeng** (曾怡碩) is an Associate Research Fellow in the division of cybersecurity and decision-making simulation at the Institute for National Defense and Security Research (INDSR), a non-partisan research organization affiliated with Taiwan's Ministry of National Defense. He also lectures at National Defense University and Tamkang University as an adjunct assistant professor. He holds a B.A. in finance from National Taiwan University and a Ph.D. in Political Science from the George Washington University in the United States. Dr. Tzeng has been tasked with research on Chinese influence campaign, digital resilience, cyber warfare, and AI in defense.

**Min-yen Chiang** (江旻諺) is the Deputy Director for Economic Security at the Research Institute for Democracy, Society, and Emerging Technology (DSET), where he leads open-source intelligence (OSINT)–based policy research with a focus on Taiwan. His work explores critical supply chain security issues amid the ongoing U.S.-China tech rivalry. Chiang's recent publications include The Remote Poaching Model, which analyzes the entanglement between Taiwan's semiconductor industry and Huawei's

shadow supply chains, as well as studies on China's industrial policies for legacy chip manufacturing. He has also spent years advocating for reforms to strengthen Taiwan's economic security framework. Chiang is currently pursuing a Ph.D. in Political Science at Georgia State University and serves as a non-resident fellow at the Taiwan Economic Democracy Union.

**Federica Bagna** was an intern at the Institute for Security and Development Policy's Stockholm Taiwan Center (STC). She graduated from the University of Milan with a Master´s Degree in International Politics and Regional Dynamics, completing part of her studies at Xi'An Jiaotong Liverpool University in Suzhou, China. She also holds a Bachelor´s Degree in Linguistic and Cultural Mediation, specializing in Chinese and English. Her research interests center on international law, policy analysis and East Asian Studies, with a particular focus on Cross-Strait relations and regional cooperation.

# Introduction: Taiwan at the Center of the Hidden War for Technology

*Niklas Swanström and Yi-Chieh Chen*

In an era where technological supremacy increasingly determines national power and economic prosperity, the battleground for competitive advantage has shifted from traditional military theaters to research laboratories, corporate boardrooms, and academic institutions. This transformation has created new vulnerabilities that nation-states must address while maintaining the openness necessary for innovation to flourish. Taiwan, positioned at the epicenter of global technology production and caught between its democratic values and the strategic pressures of cross-Strait relations, offers a unique lens through which to examine these challenges.

## The New Landscape of Technological Competition

The contemporary security environment has fundamentally altered the relationship between research, innovation, and national security. Unlike previous eras where military and civilian technologies operated in largely separate spheres, today's technological ecosystem is characterized by dual-use capabilities that blur the lines between commercial innovation and national defense applications. Artificial intelligence (AI) algorithms developed for consumer applications can enhance military surveillance systems; semiconductor manufacturing techniques that power electronic devices also enable advanced weapons systems; and cybersecurity research that protects commercial networks can be weaponized for state-sponsored attacks and intelligence operations.

This convergence has created what scholars and policymakers increasingly recognize as a "hidden war"—a sustained campaign of technology acquisition that operates below the threshold of traditional conflict, but with equally profound implications for national security and economic competitiveness.

The stakes in this competition are particularly high for Taiwan, whose economic model has long depended on technological innovation and whose geopolitical position makes it both a target and a strategic asset in the broader technological rivalry between democratic and authoritarian systems.

## Taiwan's Unique Position and Vulnerabilities

Taiwan's role in the global technology ecosystem extends far beyond what its physical size would suggest. It serves as a critical node in global semiconductor production. Taiwan today houses the world's most advanced chip manufacturing facilities and maintains technological capabilities essential to industries, ranging from consumer electronics to defense systems. This technological prominence, however, has made Taiwan a prime target for intelligence gathering and technology transfer efforts by state and non-state actors seeking to access its innovations and expertise.[1]

The complex nature of cross-Strait relations compounds Taiwan's challenge. The People's Republic of China's (PRC) claims on Taiwan create a unique security environment where traditional distinctions between foreign and domestic threats become blurred. Since 2020, 159 individuals have been prosecuted in Taiwan for espionage on behalf of China, highlighting the growing difficulty in distinguishing friends from foes within Taiwanese society.[2] Economically, the extensive economic ties between Taiwan and mainland China, including significant investment flows and personnel exchanges, create pathways for both legitimate business activities and potential intelligence operations. These situations require Taiwan to develop sophisticated approaches to technology protection that distinguish between legitimate cooperation, and activities in the realms of economic competitiveness and research and innovation security that pose national security risks.

## The Evolving Threat Landscape

The PRC's approach to technology acquisition represents a systematic and multi-faceted campaign that leverages various channels and methodologies. Foreign direct investment is one pathway, allowing Chinese entities to

access Taiwanese companies and their technological capabilities. Corporate espionage activities target proprietary technologies and trade secrets across multiple sectors. Talent recruitment programs aim to attract Taiwanese researchers and engineers to mainland China, potentially taking critical knowledge. The military-civil fusion strategy seeks to integrate civilian technological advances into defense capabilities, making any technology transfer potentially relevant to military applications.

This multifaceted approach presents particular challenges for Taiwan's security apparatus. Traditional counterintelligence measures designed to address conventional espionage activities may be inadequate for addressing the more subtle forms of technology transfer that occur through seemingly legitimate business and academic exchanges. The challenge is further complicated by the need to maintain Taiwan's openness to international collaboration and investment, which is essential to its continued technological leadership.

## Sectoral Vulnerabilities and Strategic Implications

The scope of Taiwan's technological vulnerabilities extends across multiple critical sectors. This volume focuses on AI, semiconductor manufacturing, cybersecurity, and academic exchanges across the Taiwan Strait. Taiwan's research institutions and technology companies in AI have developed significant capabilities in machine learning, computer vision, and other AI applications. However, foreign entities are increasingly seeking these same capabilities to enhance their AI development programs or counter Taiwan's development. The semiconductor supply chain represents Taiwan's most strategically important technological asset, with Taiwan Semiconductor Manufacturing Company (TSMC) and other Taiwanese firms controlling significant portions of global advanced and mature chip production. Nonetheless, Taiwanese firms focusing on mature chip manufacturing have been struggling to compete with their Chinese counterparts.

Information security and cybersecurity represent another critical domain where Taiwan faces ongoing challenges. As cyber threats become more sophisticated and state-sponsored, Taiwan's cybersecurity sector has

developed advanced defensive capabilities. However, the same expertise that enables Taiwan to defend against cyberattacks also makes its cybersecurity professionals and companies attractive targets for foreign intelligence services. In addition to this, cyberattacks targeting Taiwan's critical infrastructure and industries, such as telecommunication, information technology companies and hospitals, have been urgent concerns. These attacks not only jeopardize Taiwan's traditional conception of national security, but also its capabilities in safeguarding public welfare.

## The Innovation Security Dilemma

Taiwan's experience illustrates the broader challenge that many nations face in balancing the requirements of national security with the needs of innovation ecosystems. Innovation thrives in environments characterized by openness, collaboration, and the free flow of ideas and talent. However, these same characteristics that enable innovation also create vulnerabilities that can be exploited by hostile actors seeking to acquire sensitive technologies.

This dilemma is particularly acute for Taiwan given its position in the global technology ecosystem. Taiwan's technology sector depends heavily on international collaboration, foreign investment, and access to global talent pools. Overly restrictive security measures could undermine these collaborative relationships and damage Taiwan's technological competitiveness. However, insufficient security measures could result in the loss of critical technological advantages essential to Taiwan's national security and economic prosperity.

Taiwan's approach to addressing these challenges has involved the development of increasingly sophisticated legal and policy frameworks designed to protect sensitive technologies while maintaining the openness necessary for continued innovation. These frameworks must address multiple dimensions of the technology security challenge, including foreign investment screening, export controls, counterintelligence activities, and academic security measures.

The construction of these frameworks has required Taiwan to learn from the experiences of other nations while adapting approaches to its unique circumstances. European countries and the United States (U.S.) have implemented various measures to address similar challenges with different success rates, but Taiwan's particular geopolitical situation and economic structure require tailored solutions that may not be directly transferable from other contexts.

## International Dimensions and Cooperation

Taiwan's technology security challenges cannot be addressed in isolation. The interconnected nature of global technology supply chains means that vulnerabilities in one location can have cascading effects across the entire system. This reality has led to increasing recognition of the need for international cooperation in addressing technology security challenges, even as Taiwan's unique diplomatic status complicates its participation in some multilateral frameworks. This is also one of the reasons why China is actively opposing any internationalization of Taiwan-related issues, and aims at closing Taiwan's engagement multilaterally.

The development of informal cooperation mechanisms and partnerships with like-minded nations has therefore become an important component of Taiwan's approach to technology security. These relationships enable information sharing, best practice development, and coordinated responses to common threats while respecting the political sensitivities surrounding Taiwan's international status.

## The Human Dimension

One of the most challenging aspects of Taiwan's technology security environment is the human dimension. The mobility of skilled professionals, researchers, and entrepreneurs is essential to maintaining Taiwan's technological dynamism. However, this same mobility creates opportunities for the unauthorized transfer of sensitive knowledge and technologies.[3] Taiwan must develop approaches that can protect against hostile talent acquisition while maintaining its attractiveness as a destination for international talent

and preserving the professional mobility that its own citizens expect.

The challenge is further complicated by the cultural and linguistic ties that many Taiwanese professionals have with mainland China. These connections, while often personal and benign, can create vulnerabilities that hostile intelligence services may seek to exploit. Taiwan's approach to this challenge must be nuanced enough to distinguish between legitimate personal and professional relationships and activities that pose genuine security risks.

## Lessons for the International Community

Taiwan's experience in addressing technology security challenges offers valuable lessons for other nations facing similar dilemmas. The island's unique position as both a technology leader and a target of systematic technology acquisition efforts provides insights into the evolving nature of technological competition and the policy responses that may be most effective in addressing these challenges.

The lessons from Taiwan are particularly relevant for other technologically advanced nations that maintain significant economic relationships with China while seeking to protect their technological advantages. Taiwan's experience demonstrates both the challenges and opportunities inherent in developing comprehensive approaches to technology security, which can address multiple threats in different sectors while maintaining the openness necessary for continued innovation.

## Scope and Structure of This Volume

This edited volume presents a comprehensive examination of Taiwan's approach to technology security challenges across multiple sectors and policy domains. The contributors, drawn from academic institutions and government agencies, offer diverse perspectives on the challenges Taiwan faces and the strategies it has developed to address them.

The volume is structured to provide both sectoral analysis and cross-cutting themes that illuminate the broader patterns of Taiwan's technology security

challenges. Individual chapters examine specific sectors including AI, semiconductors, cybersecurity, and academic exchanges. The contributors have sought to present a balanced assessment that acknowledges both the successes and limitations of Taiwan's approach while identifying areas where further development may be necessary.

## Looking Forward

This volume serves as a pilot project for examining technology security across the Taiwan Strait. Much attention has been given to AI, semiconductor manufacturing, and cybersecurity in the context of China leveraging geographical proximity and cultural-linguistic similarities to gain access to Taiwanese businesses, academics, and sensitive information. However, many other critical areas remain under-explored. These include technology in the defense industry, satellites systems, agricultural innovation, and the broader challenges of technological development.

Taiwan has committed significant resources to advancing its technological capabilities while strengthening legal frameworks to protect its innovations. These efforts are crucial to maintaining Taiwan's resilience against external pressures and reinforcing its position as one of the global tech leaders. However, advancing technological development requires international collaborations, which remain difficult given Taiwan's unique political position in the international community.

The challenges Taiwan faces are not only about guarding against China's espionage, but also about overcoming the exclusion from the international community. A closer look at Taiwan's experience can offer valuable insights into how democratic nations can manage technological development under the growing pressures of authoritarian regimes. It highlights not just which technologies deserve focus, but also how to foster meaningful international cooperation in a constrained geopolitical environment.

## Endnotes

1 Niklas Swanström and Viktor Šimov, "Safeguarding the Global Chip Supply: Lessons from PRC's Technology Acquisition Tactics in Taiwan," Institute for Security and Development Policy, July 2025, https://www.isdp.eu/publication/safeguarding-the-global-chip-supply-lessons-from-prcs-technology-acquisition-tactics-in-taiwan/.

2 吳書緯，"國安局：2020年至今共諜案起訴 現退役軍人占6成" [National Security Bureau: 60% of Communist spy cases prosecuted since 2020 are from current veterans], Central News Agency, April 8, 2025, https://www.cna.com.tw/news/aipl/202504080046.aspx.

3 See n .1.

# 1. Cross-Strait Academic Exchanges: Balancing Collaboration and National Security

*Yu-chung Shen*

## Introduction

Since the end of the pandemic and the beginning of Xi Jinping's third term (starting in 2022), cross-Strait relations have undergone significant changes. The Chinese Communist Party (CCP) has adopted a multifaceted approach to pressure Taiwan (Republic of China) regarding its sovereignty. In addition to traditional military threats and economic coercion, it has recently intensified efforts in united front operations and infiltration into various aspects of Taiwanese society.

From the perspective of cross-Strait exchanges—spanning academia, science and technology, religion, culture, and other fields—Taiwan's position is to promote healthy and orderly exchanges based on the preservation of national sovereignty and its liberal democratic constitutional system. For China, however, such exchanges are carried out under the premise of the "One China Principle" or the "1992 Consensus." These exchanges are seen as tools aimed at eliminating the sovereignty of the Republic of China and achieving unification and integration under Beijing's leading.

This chapter discusses the changes in cross-Strait exchanges in recent years and then analyzes how scientific and technological exchanges between Taiwan and China can be balanced with national security.

## Changes in Cross-Strait Relations: China's "Two-Handed Strategy"

Cross-Strait exchanges took on a new dynamic after the end of the COVID-19 pandemic. From Beijing's perspective, the conclusion of the pandemic coincided with Xi Jinping beginning his third term as China's leader in 2022, marking a period of increased centralization and political tightening. Xi's Taiwan policy has emphasized "integration," with a significant expansion of united front efforts across various sectors, particularly in religion, sports, and academia.

On the Taiwan side, Lai Ching-te was elected president in 2024 and has since taken office. His administration seeks to promote healthy and orderly exchanges with China, while also adopting a more de-risk approach to managing the CCP's united front tactics aimed at Taiwan.

Overall, the CCP has intensified its "two-handed strategy" toward Taiwan—using a hardline approach to oppose independence, while employing softer tactics to promote unification. On the hardline front, over the past few years, the CCP has increasingly deployed large numbers of military aircraft and naval vessels to harass Taiwan, conducted large-scale joint military operations and exercises, and engaged in gray-zone maritime conflicts with greater frequency. In addition, it has introduced legal measures aimed at deterring Taiwan independence, attempting to create the illusion of jurisdiction over Taiwan through "lawfare."

On the international stage, Beijing continues to constrict Taiwan's diplomatic space by invoking United Nations General Assembly Resolution 2758 and promoting its "One China Principle." In short, the hard approach has involved a significant escalation in the use of military force, legal tactics, and international pressure to suppress Taiwan independence.

On the softer front, the CCP has also intensified its efforts to engage with and exert united front influence over Taiwan, using the neighboring province of Fujian as a base to promote the idea of "unification through

integration." This strategy involves collaborating with local partners in Taiwan to deepen social infiltration and sow division. Various exchanges under the banners of sports, religion, culture, and academia have been carried out extensively, though many of these activities serve as vehicles for united front work.

In response to this dual strategy, President Lai announced a 17-point national security strategy on March 13, 2025, with the primary goals of countering united front efforts and preventing infiltration. Overall, Taiwan's guiding principle for cross-Strait exchanges—particularly in the cultural and educational fields—is to ensure "depoliticization" and "risk reduction," thereby enabling exchanges to proceed in a simple and orderly manner. Under this principle, future cultural and academic exchanges between the two sides must also strike a balance between openness and national security risk management.

## Academic Exchanges: The CCP's Tools for United Front Work and Sharp Power Toward Taiwan

In the realm of academic and scientific exchanges, China has leveraged such interactions not only to enhance its own national power, but also as a component of its united front tactics toward Taiwan. Moreover, cultural and educational exchanges have become emblematic of China's exercise of "sharp power" on the international stage. A notable example is the Confucius Institutes, which once attracted global attention. Initially promoted by China as a key instrument for expanding its soft power, these institutes are now regarded by many democratic countries as a symbol of China's sharp power in action, leading to widespread termination of partnerships. The fundamental difference between soft power and sharp power lies in intent: while soft power seeks attraction and persuasion, sharp power aims at infiltration and the erosion of the target country's autonomy. Nye (2018) pointed out that when a Confucius Institute crosses the line and tries to infringe on academic freedom (as has occurred in some instances) it should be treated as sharp power.[1]

By this standard, the CCP uses cultural and educational exchanges as a means of infiltrating and undermining target countries in order to achieve its political objectives. Taiwan, in this context, can be considered the primary target of China's sharp power operations.

Cultural and educational exchanges are not only manifestations of sharp power but also tools the CCP uses to advance its political objectives by controlling the degree of openness in such exchanges. For example, in 2020, the CCP unilaterally suspended the enrollment of mainland Chinese students in Taiwanese institutions, a policy that remains in effect. In contrast, Taiwanese students are still permitted to study in mainland China, and Taiwan continues to maintain an open stance. This has resulted in a clear imbalance: while Taiwanese students continue to go to China for education, the number of mainland Chinese degree students studying in Taiwan has dropped to zero.

Moreover, there have been instances in the past where the CCP required Taiwanese universities to sign a "One China" pledge as a precondition for engaging in academic exchange. These cases illustrate how the CCP formulates policy tools that frame academic exchange not only as a component of its united front work toward Taiwan, but also as a form of sharp power aimed at achieving its political goals.[2]

Programs such as the "Thousand Talents Plan" and the "Changjiang Scholars Program" exemplify how the CCP uses the guise of scientific and academic exchange to attract foreign scholars and bolster China's research capabilities. These initiatives often target experts in critical and core technologies, highlighting the CCP's strategy of leveraging academic collaboration to overcome technological bottlenecks and, in turn, undermine Taiwan's national security.

In a report to the legislature released in 2024, Taiwan's Investigation Bureau noted that the CCP has recently intensified its efforts to recruit Taiwanese technological talent and steal sensitive technological know-

how.[3] In the context of the ongoing U.S.-China trade and tech wars and the resulting global supply chain restructuring, the CCP has sought to build an autonomous semiconductor supply chain to circumvent U.S. technological restrictions. As part of this effort, it has actively infiltrated Taiwan's high-tech sector through tactics such as "fake cooperation, real control," "fake dispatch, real R&D," "fake representation, real localization," and "fake investment, real shareholding." The report also highlights the establishment of shell companies to handle insurance and salaries for Taiwanese employees, thereby facilitating the poaching of high-tech talent and the theft of commercial secrets and critical technologies—actions that undermine Taiwan's economic competitiveness.

The same report further reveals that the CCP also uses cultural exchanges to mask its united front agenda. By capitalizing on the geographical proximity and shared historical, cultural, and linguistic ties between Taiwan and China, the CCP promotes a narrative of cultural affinity. It manipulates the concept of diaspora culture to shape identity, emphasizing that Taiwan's religious and ethnic roots originate from China as a means of advancing its political influence.

## Taiwan: Management and De-Risking

In response to academic exchanges with China that carry risks of sharp power, united front influence, and infiltration, Taiwan manages cross-Strait academic engagement from the perspective of national security. The core principles guiding this approach are the de-politicization of cross-Strait academic exchanges and the mitigation of associated risks. Several concrete measures include:

1. All bilateral cooperation agreements between universities and research institutions across the Taiwan Strait must receive prior approval from relevant government authorities to ensure proper risk management. Agreements signed without such approval are considered invalid, and institutions that unilaterally enter into unauthorized agreements may face penalties, including reductions in government funding or subsidies.

2. For national security reasons, Taiwan restricts academic exchanges with China on certain sensitive topics. A cross-ministerial task force has been convened by the government to designate a list of "National Core Technologies," aimed at ensuring that critical technologies are not leaked through academic or research collaboration, thereby preventing national security vulnerabilities.

   The definition of "National Core Technologies" is based on Article 3, Paragraph 1 of the National Security Act. It refers to technologies that, if leaked to foreign entities or hostile forces abroad, would significantly harm national security, industrial competitiveness, or economic development. Such technologies must also meet at least one of the following criteria:

   (1) They are subject to international treaties, necessary for national defense, or essential for the protection of critical national infrastructure;

   (2) They enable Taiwan to develop leadership-level technologies or significantly enhance the competitiveness of key industries.

   In 2023, the government published the first list of core technologies, identifying 22 items. In 2024, an additional 10 items were added, bringing the total to 32, across five major sectors:

   - National defense technology
   - Space technology
   - Agricultural technology
   - Semiconductor technology
   - Information and communication security

   Furthermore, the National Security Act stipulates harsher penalties for acts that infringe upon trade secrets related to these core technologies. In addition, any personnel funded, subsidized, or commissioned by the government to work on projects involving core technologies must undergo a vetting process before traveling to mainland China.

3. In addition to safeguarding critical technologies, Taiwan has expanded restrictions to prohibit specific institutions as exchange partners. In line with the practices of many democratic countries, Taiwan prohibits academic exchanges with certain Chinese institutions that have special affiliations or strategic missions—such as the so-called "Seven Sons of National Defense" (國防七子). This measure aims to ensure that academic collaboration does not contribute to the enhancement of the CCP's military capabilities.

   On February 28, 2025, Taiwan's Education Minister Cheng Ying-yao (鄭英耀) said that universities in Taiwan are prohibited from engaging in exchanges with seven universities under China's Ministry of Industry and Information Technology (MIIT) due to concerns that key Taiwanese technologies could be "stolen."

Military-industrial universities refer to higher education institutions affiliated with China's defense science, technology, and military industrial systems. In 1993, following years of restructuring and institutional consolidation, seven universities under the Commission for Science, Technology and Industry for National Defense (COSTIND) of the People's Liberation Army were collectively designated as the "Seven Sons of National Defense." These institutions include:

- Harbin Institute of Technology
- Harbin Engineering University
- Beihang University (Beijing University of Aeronautics and Astronautics)
- Beijing Institute of Technology
- Northwestern Polytechnic University
- Nanjing University of Aeronautics and Astronautics
- Nanjing University of Science and Technology

In 2008, the responsibilities of COSTIND were absorbed into the newly established Ministry of Industry and Information Technology (MIIT), and the "Seven Sons of National Defense" were subsequently placed under MIIT's jurisdiction. According to research by the Harvard Kennedy School,

the ways in which these seven schools are "directly subordinate" to the MIIT may be different for different universities. However, the relationship includes at least three aspects: funding; personnel appointments; and high-level guidance, approvals, and meetings.[4] Some researchers even refer to the Seven Sons as the "principal force behind innovation in military-civil cooperation."

According to the China Defense Universities Tracker maintained by the Australian Strategic Policy Institute (ASPI), all of the "Seven Sons of National Defense" are rated as "very high risk" in terms of potential involvement in espionage or other improper activities.[5] This highlights that the practices of these Chinese universities have gone far beyond the scope of normal academic exchange.

Given the significant military-industrial background of the Seven Sons, the European Union (EU) has also begun reviewing and cataloging collaborative projects involving these institutions. The EU over the past decade has funded at least 14 projects for €26 million that worked with Chinese universities deemed "high-risk" by experts. Eight of these projects are still ongoing. The research topics ranged from decarbonization, climate modeling and heating and cooling technology to antennas and motor propulsion technology. Some other democratic countries or regions have also taken concrete steps to prohibit collaboration with the "Seven Sons of National Defense." For example, Flanders in Belgium has explicitly banned cooperation with these institutions. The Flemish government (Belgium) has also revealed in parliament that it is banning new collaborations with China's "Seven Sons of National Defense" universities to prevent potential misuse of civilian information or espionage by Chinese researchers.

## Conclusion : De-risked Academic Exchange

Since the Democratic Progressive Party (DPP) came to power in 2016, Taiwan has undertaken a comprehensive review of its exchanges with China—including those in the economic, cultural, and academic spheres. In light of the CCP's increasingly aggressive united front tactics and

infiltration efforts toward Taiwan, de-risked engagement has become a key guiding principle of current policy.

From an objective perspective, the number of individuals entering Taiwan from China for cultural and educational activities has steadily declined since 2016. A decade ago, these figures exceeded 30,000 annually; in the post-pandemic period, they have dropped to just 2,000 to 3,000. For trends in academic and cultural exchanges, refer to Table 1 and Figure 1 as follows.

| Time | Application | Approval | Entry |
|---|---|---|---|
| 2014 | 29664 | 27987 | 26855 |
| 2015 | 35762 | 35008 | 34316 |
| 2016 | 34085 | 33471 | 33885 |
| 2017 | 27778 | 26966 | 27168 |
| 2018 | 21800 | 21305 | 21928 |
| 2019 | 17976 | 17827 | 18567 |
| 2020 | 2629 | 2770 | 60 |
| 2021 | 27 | 28 | 26 |
| 2022 | 292 | 116 | 55 |
| 2023 | 4694 | 3444 | 2693 |
| 2024 | 3787 | 3345 | 2526 |

Table 1. **Number of entrants for academic and cultural exchange**

Source: Tourism Statistics Database of the Tourism Administration, https://stat.taiwan.net.tw/.

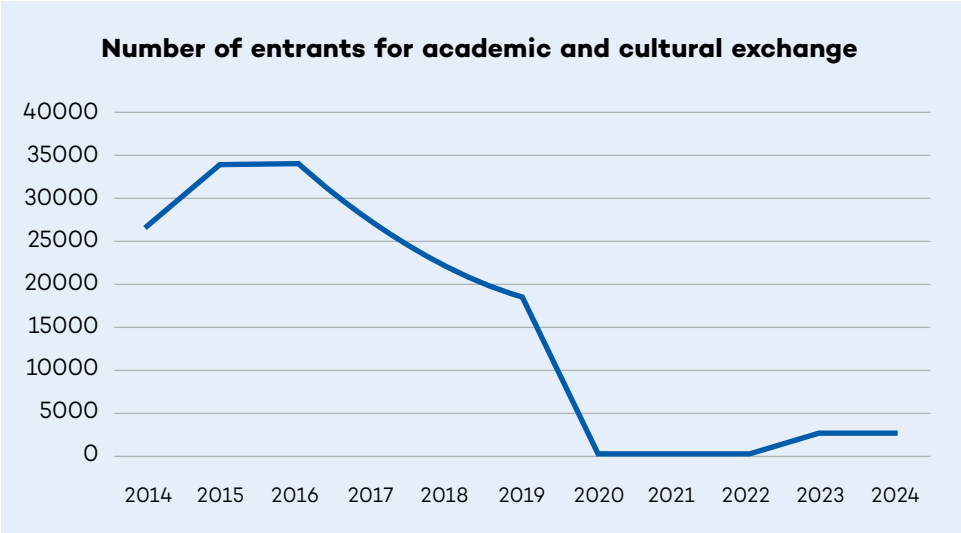


Figure 1. **Number of entrants for academic and cultural exchange**

Source: Tourism Statistics Database of the Tourism Administration, https://stat.taiwan.net.tw/.

On March 13, 2025, President Lai held a press conference following a high-level national security meeting and announced 17 major strategies to respond to the national security and united front threats. One of these 17 strategies is to prevent national security risks caused by academic or education exchanges. President Lai pointed out that political interference from China and the resulting risks to national security should be avoided in cross-Strait exchanges. This includes the review and management of religious, cultural, academic, and education exchanges, which should in principle be depoliticized and de-risked so as to simplify people-to-people exchanges and promote healthy and orderly exchanges.

## Endnotes

1 Joseph S. Nye Jr., "How Sharp Power Threatens Soft Power," *Foreign Affairs*, January 24, 2018, https://www.foreignaffairs.com/articles/china/2018-01-24/how-sharp-power-threatens-soft-power.

2 Cheng-Yi Lin, "Taiwan and American Perception and Analysis of China's Sharp Power," *Security and Intelligence Studies* 4, no. 2 (2021): 1–47.

3 Public Affairs Office, Ministry of Justice Investigation Bureau (Taiwan, Republic of China), "法務部調查局同步偵辦「中」企非法在臺挖角高科技人才案" [The Ministry of Justice's Investigation Bureau is also investigating a case of Chinese companies illegally poaching high-tech talent in Taiwan], March 28, 2014, https://www.mjib.gov.tw/news/Details/1/1083.

4 Dan Murphy, "The Seven Sons of National Defense," Ash Center for Democratic Governance and Innovation, Harvard Kennedy School, November 2024, https://rajawali.hks.harvard.edu/wp-content/uploads/sites/2/2024/11/240948-HKS-Occasional-Seven-Sons-FINAL-11-19.pdf.

5 陳穎萱, "中共利用學術合作促進軍事現代化" [China Manipulates International Academic Cooperation for Its Military Programs], *Biweekly Report of National Defense and Security*, no. 44 (2021): 41–46, https://indsr.org.tw/respublicationcon?uid=12&resid=840&pid=1246.

# 2. China's Military-Civil Fusion Strategy for AI Technology

*Shiow-Wen Wang*

## Introduction

Artificial intelligence represents a core area of technological and strategic competition between China and the United States (U.S.). While AI is reshaping economic systems and social governance, its military applications may redefine global power balances. The Chinese government views AI not only as a frontier technology but as a strategic lever to achieve asymmetrical superiority over advanced powers like the U.S. and Europe. This ambition is evident in China's national policies and its comprehensive, whole-of-society approach to AI advancement.[1]

## Current Status of AI Development in China

China is currently the only country capable of competing with the U.S. in the field of AI. On January 21, 2025, Chinese AI startup DeepSeek released its large language model (LLM), DeepSeek-R1. Its low cost and high performance were widely credited with contributing to a 17 percent drop in NVIDIA's stock price, eliminating approximately $589 billion in market value in a single day.[2] This milestone highlighted the narrowing AI gap between the two powers, particularly in the domain of LLMs.[3]

According to the China Academy of Information and Communications Technology (CAICT), by July 2025, a total of 3,755 LLMs had been released globally, with Chinese firms accounting for 1,509 of them.[3] China is home to over 5,100 AI companies (15 percent of the global total), and 71 of the world's 271 AI unicorns (26 percent).[4]

Key features of China's AI development model include:

1. **Top-Down National Strategy:** The government has adopted a "whole-of-nation" approach to steer and promote AI development. The *New Generation Artificial Intelligence Development Plan* (2017) set phased goals to make China a global AI innovation hub by 2030. Significant government funding and resources have been allocated to narrow the gap with the U.S..

2. **Municipal Competition:** Municipal governments actively encourage AI industry growth, with cities such as Beijing, Shanghai, Hangzhou, and Shenzhen fostering numerous AI startups.

3. **Talent Cultivation:** AI education begins as early as primary school, while leading universities like Peking and Tsinghua produce world-class AI talent. Whether these individuals remain in China or pursue careers abroad, they have made significant contributions to global AI innovation.[5]

4. **Tech Industry Integration:** Tech giants such as Huawei, Alibaba, and Baidu have launched robust AI initiatives and provided open cloud computing platforms to accelerate research and application development.

In short, China has built a comprehensive AI ecosystem supported by strong policy guidance and financial investment. Unlike the U.S., which benefits from a free-market system with abundant venture capital for early-stage innovation, China has focused primarily on AI applications across various domains. U.S. export restrictions on advanced AI chips and equipment have also spurred China to pursue domestic alternatives and cost-effective innovation, as evidenced by DeepSeek's performance.

## AI Military Applications of the People's Liberation Army

China recognized AI's military potential early and regards it as a core component of "new-type combat capabilities." The *New Generation AI Development Plan* explicitly promotes AI integration into military-civil

fusion (MCF) initiatives, highlighting its role in command-and-control systems, military simulations, and autonomous platforms.[6]

China is well-positioned to develop AI-enabled military systems. It ranks second globally in overall AI capability, behind only the U.S., and leads in several enabling technologies. It controls 80 percent of the global civilian drone market, operates the Beidou satellite navigation system, leads in 5G infrastructure, and possesses a comprehensive AI industrial supply chain from LLMs to robotics. Its state-owned defense conglomerates are now integrating AI into weapon development and manufacturing—particularly in aerospace, aviation, and maritime domains.

If China were to achieve large-scale production of AI-enabled weapons—such as loitering munitions, unmanned platforms, and robotic forces—at low cost with high precision, the People's Liberation Army's (PLA) "intelligentized" operational capability would likely expand.[7]

The PLA's intelligentization efforts currently emphasize four core domains:[8]

1. Situational awareness and intelligence fusion
2. Dynamic communications and battlefield networking
3. Intelligent decision-making and command and control system
4. Unmanned systems and swarm operations

The PLA has fielded AI-enabled systems such as the **"War Brain"** (戰顱) wargaming platform and **"Thousand-Hand Guanyin"** （千手觀音） communications system—reportedly a counterpart to the U.S. JTACS., alongside AI for voice recognition, image analysis, autonomous weapons, and robotic wolves and dogs. The PLA also built the world's first military 5G network with China Mobile, capable of linking over 10,000 robots for coordinated operations.[9] Additionally, the PLA has leveraged Meta's open-source LLaMA to build its proprietary **"ChatBIT"** model and integrated DeepSeek LLMs into its military hospital networks.[10]

In practice, both the U.S. and China have recognized that the scope of AI military applications far outpaces the capabilities of traditional defense industries, thereby necessitating innovation from private-sector companies. This trend was evident at the military exposition held in Beijing in May 2025, where over 500 civilian companies showcased more than 3,000 products and solutions. Among these were AI-powered military applications proposed by private firms, including intelligent command-and-control systems, military training assistance models, LLMs for decision-making, and combat simulation and exercise systems.[11] It is likely that the PLA will further deepen and widen its MCF with civilian AI companies in the future.

## How Does the PLA Promote Military-Civil Fusion in AI?

There are multiple approaches through which the PLA promotes the integration of AI technologies from the civilian sector:

### 1. Establishing Hubs within Innovation Parks

In late 2016, the PLA established the "Zhongguancun Military-Civilian Integration and Coordination Platform" in Haidian District, Beijing, to align civilian technologies and products with military needs.[12] Haidian is home to 37 universities—including Peking University and Tsinghua University—92 national key laboratories, and 96 national research institutes. The region hosts over 10,000 AI scholars, including more than 100 top global AI researchers listed in the AI 2000 ranking.[13] The PLA's presence here allows it to stay abreast of cutting-edge research and industrial applications while fostering collaboration with academia, research institutions, and AI companies.

### 2. Procuring Civilian AI Products That Meet Military Requirements

Private companies must typically obtain military procurement supplier certification to bid for defense contracts. However, according to U.S. officials, the AI firm *DeepSeek* has appeared in more than 150 procurement documents related to the PLA and affiliated entities and has reportedly provided services to at least one PLA research institute.[14]

### 3. Collaborating with Tech Giants

The PLA has strengthened partnerships with leading tech companies. For instance, in 2018, Baidu and the 28th Research Institute of the China Electronics Technology Group Corporation jointly established the "Laboratory for Intelligent Command and Control Technology," which focuses on AI applications for military command systems. Huawei has collaborated with the PLA's former Strategic Support Force's "University of Information Engineering" on a 5G research project. It has been reported that a PLA-affiliated university lab has tested military AI systems using Baidu's *ERNIE Bot* and iFlytek's *Xinghuo* (Spark) cognitive LLM.

### 4. Investing in Private AI Startups

Many private AI companies in China are startups. State-owned defense enterprises (SOEs) often engage in early-stage investments through venture capital or through equity acquisitions under a "mixed-ownership" model to bring these startups into their portfolios. For example, military SOEs have invested in Beijing-based startup *Baiyang AI* (白杨智能), which focuses on technologies such as deep reinforcement learning and decision-making LLMs. This company has been involved in several national defense intelligence projects. Its team includes alumni from major high-tech firms like Alibaba and research institutions such as the Chinese Academy of Sciences, with many members having graduated from Tsinghua University, Peking University, and the Hong Kong University of Science and Technology.[15]

### 5. Launching Major Research Projects to Attract Academic and Corporate Participation

The Central Military Commission's Equipment Development Department and Science and Technology Committee provide subsidies to universities to conduct research in defense-related technologies. Moreover, the Defense Science and Technology Industry Bureau's cooperation programs, related defense laboratories, and shared military-civil platforms also encourage participation from academia and enterprises alike.

6. **Expanding Talent Exchange with the Private Sector**
   The PLA has broadened its recruitment of civilian personnel, such as postdoctoral researchers at military research institutes. Retired military science and technology personnel are also encouraged to join private tech firms such as Huawei, or to collaborate with private-sector R&D teams to co-author research papers and continue advancing dual-use innovations.

## Security Threats from the PLA's AI-Driven Military-Civil Fusion

The rapid advancement of AI in the PLA presents significant strategic risks. As of 2025, the PLA has deployed 24 types of unmanned systems across aerial, ground, and underwater domains. These include unmanned aerial vehicles (UAVs) such as the *Rainbow, Wing Loong*, and *WZ-8*, robotic dogs, unmanned underwater vehicles (UUVs) like the *Orca*, and platforms such as *Type 076* amphibious assault ship.

Simultaneously, China is pursuing next-generation weapons—including active phased-array radars, strategic nuclear submarines, electromagnetic railguns, laser weapons, and hypersonic missiles. In parallel, the PLA is developing a new space warfare initiative known as the "South Heavenly Gate Project" (南天門計畫), which aims to integrate space-based fighters and unmanned combat aircraft to establish space superiority. These developments could pose significant risks to cross-Strait stability and to Taiwan's security.[16]

Moreover, China is reportedly attempting to integrate generative AI into its intelligence analysis and military planning systems.[17] If successful, this could significantly enhance the PLA's ability to monitor developments across the Indo-Pacific region—particularly the Taiwan Strait, the South China Sea, and the East China Sea—formulate response strategies, and develop operational plans. AI may also accelerate the tempo of warfare, placing unmanned AI-controlled systems at the center of military operations. The PLA's Yuanhai (淵海) ship-based AI system can reportedly execute the full "threat

assessment–weapon assignment–interception" protocols in just 0.3 seconds. AI-based combat systems such as Zhanlu and Qianshou Guanyin are said to already be conducting electronic warfare operations targeting U.S. forces in the East China Sea, Yellow Sea, Taiwan Strait, and South China Sea.[18]

The PLA also conducts cognitive warfare, cyber operations, and espionage using generative AI. Numerous short videos circulating on social media exhibit identical text with varied images and propaganda narratives that clearly contradict factual information; these are likely to have been generated using AI. Furthermore, the PLA has long employed AI for persistent cyber intrusion, exploiting vulnerabilities in adversary networks around the clock. China's use of AI for espionage is also apparent in its large-scale hacking of foreign government and corporate databases, including Taiwan's National Health Insurance database and proprietary corporate data.

## Vulnerabilities in China's AI Military-Civil Fusion

Despite progress, a major vulnerability in China's AI-related MCF lies in its limited capacity to manufacture advanced AI chips domestically. Although China has made strides in designing advanced semiconductors, its manufacturing processes lag behind those of Taiwan's TSMC by two to three generations. As a result, since 2015, China has intensified efforts to recruit Taiwanese semiconductor talent and obtain trade secrets through illicit means.

Initially, Chinese firms attracted senior Taiwanese semiconductor professionals with salaries two to three times the industry average and subsequently used these hires to recruit their R&D teams. Over time, this evolved into establishing shell companies in Taiwan—often under foreign or overseas Chinese ownership—alongside using headhunting websites or employment agencies to recruit technical talent. More recently, Chinese firms have allowed Taiwanese professionals in fields such as integrated circuit (IC) design and memory technology to work remotely from Taiwan and transmit their results.[19]

In response, Taiwan's Investigation Bureau launched a dedicated task force in late 2020. As of March 2025, over 100 cases have been investigated. For instance, Chinese semiconductor giant SMIC was found to have used a Samoan shell company to establish a subsidiary in Taiwan, illicitly recruiting talent and stealing TSMC trade secrets. Those involved were successfully prosecuted in Taiwanese courts.[20] Similarly, in 2022, China's largest IC design firm, HiSilicon, was discovered to be recruiting Taiwanese engineers through its subsidiary Pengxin Micro, offering annual salaries ranging from NT$5 million (approximately $167,594) to NT$10 million (approximately $335,188).[21]

Amid a global shortage of talent in AI chip design and manufacturing, Taiwan is stepping up its efforts to safeguard its technological edge. Taiwan amended key legal frameworks in 2022:

- The Regulations Governing Relations Between the People of the Two Sides of the Taiwan Strait introduced a pre-approval mechanism for core technology talent going to China.
- The National Security Act added economic espionage clauses with penalties of up to 12 years imprisonment and NT$100 million (approximately $3,351,880) in fines.[16]
- In December 2023, the Executive Yuan began publishing a "List of National Core and Critical Technologies" to better protect industrial competitiveness and national security.

Taiwanese companies have adopted multiple strategies to protect critical technologies, including:

- Implementing robust supply chain risk management systems
- Enhancing password and device access controls
- Utilizing biometric authentication
- Continuously updating cybersecurity protocols

Take TSMC as an example: the company enforces military-style management. Mobile phones are strictly prohibited inside its production facilities; internal documents are subject to tiered access controls, and engineers cannot view

actual parameters when inputting data. For suppliers, TSMC uses GPS tracking after they leave factory premises and requires them to check in within a specific time window. Moreover, project-related computers used at supplier sites are set up by TSMC personnel, ensuring suppliers have no access during sensitive operations.[22]

## Conclusion

Amid the rapid global development of AI technologies, China's military-civil fusion of AI is likely to accelerate, enabling the PLA to continue enhancing its combat capabilities. Should the Chinese Communist Party succeed in integrating various sources of intelligence—from satellite imagery to communications data and real-time battlefield dynamics—into unified, AI-enabled decision-making systems, neighboring countries could face a substantial intelligence disadvantage. Furthermore, by leveraging AI across space, aviation, maritime, and cyberspace domains, China may be increasing the risk of military conflict in East Asia and the broader Indo-Pacific region. In response, democratic nations may need to accelerate their adoption of AI technologies to enhance national and regional security jointly.

## Endnotes

1 State Council of the People's Republic of China, "New Generation Artificial Intelligence Development Plan," July 20, 2017, https://www.gov.cn/xinwen/2017-07/20/content_5212064.htm.

2 Tina Teng, "Chinese startup DeepSeek rattles global markets as Nvidia shares plunge," *Euro News*, January 28, 2025, https://www.euronews.com/business/2025/01/28/chinese-startup-deepseek-rattles-global-markets-as-nvidia-shares-plunge.

3 Inskit Group, "Measuring the US-China AI Gap," Recorded Future, May 8, 2025, https://www.recordedfuture.com/research/measuring-the-us-china-ai-gap.

4 龚雯and宋晨, "我國大模型數量超1500個" [China has over 1,500 large models], *Xinhua News Agency*, July 27, 2025, http://big5.news.cn/gate/big5/www.news.cn/tech/20250727/97930c6826c147349fc068894ac6bb96/c.html.

5 Trelysa Long, "AI Is Powering the US Economy, But Who's Powering AI?" Information Technology and Innovation Foundation (ITIF), April 7, 2025, https://itif.org/publications/2025/04/07/ai-is-powering-the-us-economy-but-whos-powering-ai/.

6 State Council of the People's Republic of China, "New Generation Artificial Intelligence Development Plan," July 20, 2017, https://www.gov.cn/xinwen/2017-07/20/content_5212064.htm.

7 Shiow-Wen Wang, "An Analysis of the PLA's Accelerated Integration of AI Applications," *Biweekly Report of National Defense and Security*, no. 91 (2025): 1–6, https://indsr.org.tw/respublicationcon?uid=12&resid=3018&pid=5560.

8 Kong Guang, Wang Xin, et al., "Prospects for Intelligent Warfare Operations Systems," *Military Digest*, no. 10 (2024), http://www.c2.org.cn/h-nd-1331.html.

9 Stephen Chen, "China rolls out world's first military-proof 5G that can connect 10,000 army robots," *South China Morning Post*, December 31, 2024, https://www.scmp.com/news/china/science/article/3292490/china-rolls-out-worlds-first-military-proof-5g-can-connect-10000-army-robots.

10 Amber Wang, "China's PLA is using DeepSeek AI for non-combat support. Will actual combat be next?" *South China Morning Post*, March 23, 2025, https://www.scmp.com/news/china/military/article/3303512/chinas-pla-using-deepseek-ai-non-combat-support-will-actual-combat-be-next.

11 "从军博会看解放军如何使用AI" [How the PLA Uses AI: Insights from the Military Expo], *Sina Finance*, May 21, 2025, https://finance.sina.com.cn/jjxw/2025-05-21/doc-inexhsqh0547873.shtml?froms=ggmp.

12 Central People's Government of the People's Republic of China, "中關村軍民融合軍地對接平台啟動" [Zhongguancun Military-Civilian Integration Military-Civilian Coordination Platform Launched], December 25, 2016, https://www.gov.cn/xinwen/2016-12/25/content_5152645.htm.

13 “海淀区重磅推出“中關村AI北緯社區”打造全球人工智慧創新戰略高地” [Haidian District Launches ‘Zhongguancun AI North Latitude Community’ to Build a Global Artificial Intelligence Innovation Strategy Hub], Sina Finance, March 30, 2025, https://finance.sina.com.cn/cj/2025-03-30/doc-inermezq9360293.shtml.

14 Michael Martina and Stephen Nellis, “Exclusive: DeepSeek aids China's military and evaded export controls, US official says,” *Reuters*, June 23, 2025, https://www.reuters.com/world/china/deepseek-aids-chinas-military-evaded-export-controls-us-official-says-2025-06-23/.

15 “Breaking through the peak and ushering in a new era of intelligence,” Baiyang AI Official website, https://baiyangai.com/ (accessed November 3, 2025).

16 倪永傑, “中評月刊：智能化時代台海解決方案” [China Review Monthly: Solutions for the Taiwan Strait in the Age of Intelligence] *China Review Monthly Online Edition*, July 17, 2025, https://hk.crntt.com/doc/1070/8/9/6/107089669.html?coluid=266&kindid=0&docid=107089669&mdate=0717000727.

17 Zoe Haver, “Artificial Eyes: Generative AI in China’s Military Intelligence,” Recorded Future, June 17, 2025, https://www.recordedfuture.com/research/artificial-eyes-generative-ai-chinas-military-intelligence.

18 倪永傑, “中評月刊：智能化時代台海解決方案” [China Review Monthly: Solutions for the Taiwan Strait in the Age of Intelligence], *China Review Monthly Online Edition*, July 17, 2025, https://hk.crntt.com/doc/1070/8/9/6/107089669.html?coluid=266&kindid=0&docid=107089669&mdate=0717000727.

19 Min-yen Chiang, “The Remote Poaching Model: How China's Bitmain Acquired Taiwan's Edge - AI Chip Technology and Its Implications for Economic Security,” DSET, August 2024, https://dset.tw/wp-content/uploads/2024/08/The-Remote-Poaching-Model-3.pdf.

20 Ministry of Justice Investigation Bureau (Taiwan, Republic of China), “法務部調查局同步偵辦「中」企非法在臺挖角高科技人才案” [Ministry of Justice Investigation Bureau Simultaneously Investigates Chinese Company for Illegally Poaching High-Tech Talent in Taiwan], March 28, 2025, https://www.mjib.gov.tw/news/Details/1/1083.

21 洪友芳, “海思閃美圍堵 白手套開價千萬挖台才” [HiSilicon's Flash Memory Blockade: White Glove Offers Millions to Poach Taiwan Talent], *Liberty Times*, September 14, 2022, https://ec.ltn.com.tw/article/paper/1540089.

22 周康玉, “矽盾變局》台積電美國廠成機密破口？「新製程解碼」連核心員工都防” [Silicon Shield in Turmoil: TSMC's U.S. Plant Becomes a Security Breach? ‘New Process Decoding’ Even Core Employees Are on Guard], *The Journalist*, no. 1872-1873 (January 2023), https://new7.storm.mg/article/4689707.

# 3. China's Cyber Espionage Threat to Taiwan's Security and Industry

*Yisuo Tzeng*

## Significance of Chinese Cyber Espionage Against Taiwan

Having led China for decades in developing a comprehensive semiconductor industrial ecosystem, Taiwan has become widely recognized in recent years for its achievements in advanced chip manufacturing. The Chinese Communist Party (CCP) government has attempted to emulate Taiwan by establishing ITRI-like (Industrial Technology Research Institute) institutes and creating science and technology parks across the country in the hopes of catching up with cutting-edge technologies. Yet these efforts have largely fallen short. The CCP's overstated claims of breakthroughs in advanced chips, along with its growing reliance on espionage targeting semiconductor-related labs and firms in the U.S., the Netherlands, Japan, Taiwan and elsewhere, underscore this shortfall. Driven by the fear of being left behind in the digital age, the CCP has turned, in particular, to cyber espionage—an area in which it has outdone many others—in an attempt to narrow the technological gap and exploit the progress of leading countries in the global technology race.

The global stakes in Taiwan's semiconductor industry simply cannot be higher. With 99 percent of advanced chips manufactured in Taiwan, both U.S. Commerce Secretary Howard Lutnick and Treasury Secretary Scott Bessent have pointed out the strategic necessity of mitigating the risks of this single point of failure, not only for U.S. national security but also for the global economy.[1] Whether through tariffs or by pressing Taiwan Semiconductor Manufacturing Company (TSMC) to invest in facilities on U.S. soil, it is clear that Taiwan's semiconductor industry sits at the very top of the CCP's cyber espionage target list.

This raises the question of how Chinese hackers carry out cyber espionage and data exfiltration. Given the clandestine nature of cyber espionage and the opacity surrounding CCP sponsorship of hacktivist groups, this chapter will first address the relationship between the CCP and hacker groups. It will then outline the common strategies Chinese hackers employ to acquire information and intelligence from Taiwan. Finally, it will illuminate how Taiwan's public and private sectors tackle such a persistent security threat, with particular attention to safeguarding trade secrets in Taiwan's semiconductor industry.

## The CCP-Sponsored Cyber Espionage Ecosystem

As has been the case elsewhere around the globe, the CCP government relies on outsourcing cyber espionage operations to cybersecurity firms composed of the best in the Chinese hacktivist community. In its latest investigative report, "Countering Chinese State Sponsored Actors Compromise of Networks Worldwide to Feed Global Espionage System," the U.S. Cybersecurity & Infrastructure Security Agency (CISA) named several Chinese firms that both fit the characteristics of Advanced Persistent Threats (APT)[2] actors and have conducted malicious operations globally since at least 2021. These firms, including Sichuan Juxinhe Network Technology Co. Ltd. (四川聚信和網路科技有限公司), and Beijing Huanyu Tianqiong Information Technology Co., Ltd. (北京寰宇天穹資訊技術有限公司), have provided cyber-related products and services to China's intelligence agencies in the People's Liberation Army (PLA) and the Ministry of State Security.[3]

In contrast to the vast cyber army affiliated with Chinese militias or employed by China's Cyberspace Administration at both the central and local levels, which is primarily tasked with monitoring irregular or illegal narratives and images, these above-mentioned APT actors operate as private firms bidding on procurement contracts for cyber penetration and espionage. Their missions extend beyond stealing sensitive trade secrets; they also develop and provide technological goods and services to support the surveillance of dissidents, both within China and abroad. Therefore, public security agencies also serve as major sponsors of Chinese hackers.

Western intelligence agencies have repeatedly issued joint warnings about this practice. For instance, malicious apps developed and deployed by Chengdu Westone Information Industry Inc (成都中電科網路安全科技股份有限公司) were used by CCP public security agencies to monitor overseas Taiwanese, Uighur and Tibetan dissidents.[4]

The CCP is also well aware that Virtual Private Networks (VPNs) are used to bypass its Great Firewall, which is a system of internal censorship. To outsmart trespassers and exercise sustainable control, the CCP has sponsored certain firms to operate VPN services and thereby outsourced the espionage and censorship of information flow through these platforms. Nonetheless, the scope and scale of surveillance have gone far beyond overseas dissidents and have evolved into global surveillance. By 2019, nearly 30 percent of the world's top 100 VPNs were operated by Chinese enterprises. Among them, five firms were suspected of being owned and operated by PLA-related businessmen.[5]

In addition to outsourced espionage carried out by APT teams, the collection of personally identifiable information constitutes the cornerstone underpinning China's global surveillance. This vast pool of sensitive data pertaining to political, military and business celebrities might lead to lucrative business in data sales, intelligence collection and analysis. At the same time, this kind of centralized data storage often invites hacking, whether from outsiders seeking a free ride or from insiders seeking revenge amid internal power struggles. Incidents such as the 2019 Shenzhen Zhenhua data leak,[6] the 2022 Shanghai police data leak,[7] and the 2024 I-Soon data leak[8] expose the risks of poor data governance and protection, even when private firms manage the information. Furthermore, the latest I-Soon scandal showcased not only the shocking volume of privacy breaches and the sheer number of public-private collaborations on espionage, but also the competitive and vicious downside within China's cyber mercenary sector.

## Trends in the Ways CCP Chooses Cyber Espionage Targets

CCP cyber espionage started as part of traditional intelligence operations and remains so today. Initially, the focus was on political figures, including attempts to uncover their health conditions hidden in their financial records and hospital records. Over time, these operations became routine hacking activities, and the targets expanded to Taiwan's financial and banking systems, hospitals and emergency rescue systems. As Taiwan's semiconductor industry advances to the cutting edge, CCP-sponsored hackers have expanded their focus to trade secrets behind high-yield chip production. High-tech firms, therefore, have become top priority targets—particularly following U.S. efforts to decouple and de-risk from China. Standalone hacking rarely succeeds against the multilayered cyber defense of Taiwan's high-tech firms. Instead, compromising and intruding into cybersecurity system within the supply chain is more feasible. Therefore, CCP-sponsored hackers' focus has partially shifted from information technology to operational technology, which has laid the foundation for fierce assaults on legacy systems of critical infrastructure.

According to the latest report published by Taiwan's National Security Bureau (NSB), Chinese hackers now prioritize critical infrastructure not only for espionage but also for sabotage, creating disruptions to government and societal functions. The disruptions create psychological impacts that instill uncertainty, anxiety, fear and despair across society.[9] The CCP hopes that hybrid threats led by cyberattacks, coupled with cognitive warfare, might weaken Taiwan's will to defend the island during a Taiwan Strait contingency. Although ransomware attacks often appear to be driven solely by financial interests, they frequently serve intelligence espionage in peacetime. What seem like harmless attempts may turn into sabotage designed to generate instability and uncertainty to cripple the determination to defend Taiwan against a CCP invasion.

To disrupt and therefore intimidate and compromise Taiwanese will to fight during a contingency, CCP-sponsored hackers choose cyber espionage

targets that serve multiple purposes in peacetime. For example, cyberattacks on hospitals and emergency rescue information systems can have multiple purposes. In peacetime, they might serve to spy on high-profile individuals and exfiltrate sensitive medical and financial records for resale on the dark web. At the same time, these cyberattacks might intermittently disable hospitals' information systems to escalate gray-zone conflicts. In a contingency, however, disruption of hospitals and rescue information systems could create psychological helplessness and despair, eroding public confidence and wearing down the will to resist. Similar vicious downturns would also surface when Taiwan's governmental agencies, defense industrial bases, communications, transportation, and high-tech manufacturing sectors are under severe cyber assaults activated by China.

A combination of cognitive operations and cyber espionage is another dimension of this challenge. CCP's hackers and cyber mercenaries have been identified, exposed, prosecuted, and financially sanctioned by U.S. law enforcement agencies working together with counterparts in the Five Eyes[10] and other like-minded countries. The U.S. has successfully conducted these operations not merely by IP tracing but also by resorting to intelligence operations such as human intelligence inside China. Put simply, this is a hybrid of cyber and intelligence operations that produces psychological deterrent effects. Severe punishments, such as asset freezes on overseas accounts, have proven effective in deterring cyber mercenaries motivated by substantial profit. From late 2024 into early 2025, the CCP copied the U.S. approach and applied it to counter Taiwan's cyber force. In addition to revealing the achievement of Taiwan's cyber intrusion and espionage in China, the CCP state security agency exposed personal information about Taiwan's cyber warriors. Through this approach, the CCP agencies aimed to showcase that they employ not only cyber espionage to trace and expose those cyber professionals' personal information but also to imply that they have informants inside Taiwan's cyber force who are able to identify specific figures. By doing so, the CCP intelligence agency intends to sow distrust within Taiwan's armed forces, pressure them to search for internal moles, and weaken cohesion.

## Taiwan's Cybersecurity Measures Against Chinese Espionage

CCP's cyber espionage against Taiwan serves multiple purposes in both peacetime and times of contingency, characterized by persistent patience and a high level of sophistication in its penetration and deployment. Both U.S.'s CISA and Taiwan's NSB reports point out that CCP-sponsored APT actors would rather take a longer time to "live off the land" than take quick actions that might risk exposure.

To counter this kind of clever yet patient cyber intrusion, Taiwan's government takes precautionary and remedial measures. In addition to the Ministry of Digital Affairs calling for whole-of-society cybersecurity awareness, Taiwan's National Security Council released a new version of the National Cybersecurity Strategy to build a better coordinated whole-of-government defensive front against the CCP cyberoffensive. More than simply adopting a defensive posture, Taiwan has followed the lead of the U.S. in forward defense and the North Atlantic Treaty Organization (NATO) model of active cyber defense to cultivate a capable cyber force across both military and intelligence sectors. As revealed by China's own intelligence sector in 2025, Taiwan's cyber capabilities have reached a level that the CCP regime can no longer afford to ignore.

In the face of mounting cyber threats imposed by the CCP, Taiwan has taken a pragmatic approach—choosing not to adopt the U.S. model of integrated deterrence—recognizing that gray zone conflicts, by their nature, are extremely difficult, if not impossible, to deter through punishment alone. To counter the CCP's cyber espionage, which is inherently intelligence-driven, Taiwan employs a counterintelligence apparatus, including military counterintelligence units and the Investigation Bureau within the law enforcement sector. Taipei deploys these units forward to areas most targeted by CCP cyber espionage, in particular, the science parks that form the core of Taiwan's chip manufacturing ecosystem.

Last but not least, Taiwan embraces contingency scenarios by building digital resilience. Drawing lessons from the war in Ukraine since 2022, Taiwan has accelerated efforts to ensure continuity in the event of cyber and communication system breakdowns or manipulations. Taiwan's approach to digital resilience relies on not only data backups, backup transmission and operation apparatus, and repair and restoration capabilities, but also on ensuring the ability to maintain core government functions and societal operations even without electricity and the internet. While not yet fully ready, Taiwan is steadily developing a whole-of-society defense-resilience apparatus to withstand CCP cyber threats.

## Endnotes

1 Brent Griffiths, "The US is Exploring a Stake in Intel. It wouldn't be used 'to drum up business,' Treasury Secretary says," *Business Insider*, August 20, 2025, https://www.businessinsider.com/us-intel-trump-stake-chips-act-2025-8.

2 Advanced Persistent Threats (APT) is a type of cyberattack that aims to acquire sensitive information, conduct cyber espionage or sabotage the systems over an extended period. When the APT cyberattackers stay in the systems, they are both waiting for the timing to acquire certain information and learning the security systems. With a better understanding of the security systems, the cyberattacks can adjust their tactics accordingly.

3 "Countering Chinese State-Sponsored Actors Compromise of Networks Worldwide to Feed Global Espionage System," Cybersecurity & Infrastructure Security Agency, September 3, 2025, https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-239a.

4 英美等6國警告 中國間諜軟體鎖定台獨與西藏人權人士" [Six Countries, Including the United Kingdom and the United States, Warned That Chinese Spyware Targets Taiwan Independence And Tibetan Human Rights Activists], *Central News Agency*, April 9, 2025, https://www.cna.com.tw/news/aopl/202504090074.aspx.

5 翻牆也躲不了監控？全球百大VPN 近三成是中資" [Cannot Escape Surveillance Even If You Climb over the Wall? Nearly 30% of the World's Top 100 VPNs Are Chinese-Owned], *Liberty Times*, July 10, 2019, https://news.ltn.com.tw/news/world/paper/1302184.

6 李翰文, "深圳「振華數據」：如何看待中國國企「監控資料庫」外洩的消息" [Shenzhen Zhenhua Data: How to View China's State-Owned Monitoring Data Leak], *BBC News*, September 16, 2020, https://www.bbc.com/zhongwen/trad/chinese-news-54160466.

7 曾怡碩 and 洪嘉齡, "從上海公安資料庫遭駭竊看集中式數位監控的風險" [Risks of Centralized Digital Surveillance Revealed by Shanghai Public Security Bureau Data Leak], *Biweekly Report of National Defense and Security*, no. 59 (2022): 59–62, https://indsr.org.tw/respublicationcon?uid=12&resid=1907&pid=3311.

8 池煥衡, "NHK揭露中共網安公司I-SOON認知戰手法 外判操作爆雷不沾手" [NHK exposes the CCP's cybersecurity company I-SOON's cognitive warfare methods and outsourcing operations are not touched], *Radio Free Asia*, October 21, 2024, https://www.rfa.org/cantonese/news/china-isoon-hacker-leak-nhk-follow-cyber-espionage-industry-10212024091859.html.

9 National Security Bureau (Taiwan, Republica of China), "2024 年中共網駭手法分析"[Analysis of the CCP's Cyber Hacking Patterns in 2024], January 5, 2025, https://www.nsb.gov.tw/zh/assets/documents/新聞稿/2024年中共網駭攻擊態樣分析(報告全文)-中文.pdf.

10 The Five Eyes is an intelligence alliance composed of Australia, Canada, New Zealand, the United Kingdom, and the U.S.

# 4. Technology Controls and Supply Chain Challenges: Taiwan's Global Role in Countering China's Semiconductor Ambitions

*Min-yen Chiang*

## Introduction

In an interview with *Nikkei Asia*, Taiwanese President Lai Ching-te reaffirmed his commitment to promoting the "non-red supply chain" initiative—a strategic response to China's unfair trade practices.[1] For years, China has exploited its integration into the global free trade system to its advantage. Tactics such as intellectual property theft, product dumping in international markets, and protectionist industrial policies have propelled the rise of Chinese firms not through fair competition, but through the manipulation of global norms. Compounding the issue, the Chinese Communist Party (CCP) has increasingly blurred the line between state and enterprise by embedding Party branches within private companies.[2] This turns ostensibly private firms into instruments of state power, aligning them with the political ambitions of the CCP. In this environment, Chinese corporations often serve not just commercial functions but also as conduits for the Party's political influence abroad.

This fusion of political and economic power presents a serious challenge to both fair trade and the foundational values of liberal democracy. China's industrial policy has focused heavily on emerging technologies such as semiconductors and artificial intelligence (AI)—sectors that are central not only to economic growth but also to global geopolitical influence. In these domains, Beijing's unfair practices function as tools of strategic leverage, producing consequences that extend far beyond economic competition. Taiwan, as a global leader in semiconductor manufacturing, is uniquely

positioned to spearhead a restructuring of global supply chains to reduce reliance on authoritarian regimes. President Lai's vision for a non-red supply chain is therefore not just about enhancing economic resilience; it is a critical strategy for preserving the integrity of the international rules-based order and defending democratic systems against authoritarian encroachment.

## Taiwan: Frontline of Tech Controls and Pillar of the Global Supply Chain

Taiwan plays a dual—and deeply strategic—role in confronting China's ambitions to dominate the semiconductor supply chain. First, Taiwan is a vital enforcer of U.S.-led export control regimes. Second, it provides the global market with a reliable, efficient, and democratic alternative to Chinese technology. These roles, however, expose a tension between Taiwan's domestic policy priorities and the external pressures of an increasingly fragmented and bloc-based geopolitical environment.

On the regulatory front, the U.S. has extended the scope of its export control regime through the Foreign Direct Product Rule (FDPR), targeting advanced chip exports to China. This measure is particularly significant in restricting access to cutting-edge technologies for firms like Huawei, which maintains close ties with the People's Liberation Army.[3] Taiwan has demonstrated robust compliance, given that its semiconductor industry is heavily integrated into the global value chain and reliant on U.S.-origin technology. Observing the FDPR is thus not only a legal obligation but also a business imperative. Nonetheless, Taiwan has yet to fully embed U.S. export control logic into its domestic regulatory system. While Taiwan adheres to the spirit of the Wassenaar Arrangement and employs export licensing to curb the proliferation of dual-use technologies, it does not currently include AI chips in its controlled items list. This regulatory gap reveals a partial misalignment between Taiwan's policies and U.S. expectations in the ongoing tech war.[4]

On the industrial side, Taiwan must navigate pressure from both China's aggressive industrial policy and rising expectations from democratic allies for supply chain diversification and onshoring. The reshoring wave

in the U.S., Japan, and Europe has already drawn substantial Taiwanese investment. Taiwan Semiconductor Manufacturing Company's (TSMC) expanding presence abroad—most notably, its $165 billion investment in the U.S.—reflects this global reconfiguration. These dynamics can be conceptualized within a 2x2 matrix, with domestic policy and international trends on the horizontal axis, and regulatory framework versus industrial strategy on the vertical axis (Figure 1). Each of the four resulting quadrants represents a unique strategic scenario Taiwan must navigate. At the center lies a fundamental policy question: How can Taiwan balance three core objectives—maximizing national interest, curbing China's supply chain ambitions, and deepening partnerships with democratic allies?

| | Domestic Policy | International Trend |
|---|---|---|
| Regulatory Framework | • Wassenaar Arrangement<br>• Export Licensing Regime<br>• Outbound Investment Screening | • Export Controls on AI Chips<br>• U.S.-China Tech War |
| Industrial Strategy | • Maintaining Global Leadership in Semiconductor Manufacturing<br>• Highly Efficient and Trustworthy Partner | • China's Aggressive Industrial Policy<br>• Supply Chain Diversification and Onshoring |

Figure 1: **The Strategic Scenario for Taiwan in the Era of Tech Geopolitics**

## Building a Homegrown Export Control Regime for Taiwan

The recent Huawei-Sophgo incident, involving the AI chip company Sophgo (算能), represents one of the most serious setbacks in the U.S.' efforts to enforce its extraterritorial export control regime targeting China's advanced AI development. Reports suggest that Huawei was able to acquire more than two million advanced logic dies from TSMC through a covert network and integrate them into its Ascend 910B chips.[5] This breach created a critical loophole in Washington's broader strategy to block China's access to the computing power needed to develop state-of-the-art AI models.

TSMC had, in fact, proactively flagged Sophgo—a Xiamen-based firm—for possible downstream links to Huawei.[6] However, because Sophgo was not on the U.S. Entity List at the time, TSMC was legally permitted to supply it with advanced chips. The true vulnerability lay in the hidden relationship: Sophgo effectively acted as a front for Huawei, allowing restricted components to reach a prohibited end-user. This incident not only compromised joint U.S.-Taiwan efforts to secure the semiconductor supply chain, but also highlighted the limitations of relying solely on the Entity List as a policy tool.

Concerns about such covert networks were not new. As early as August 2024, the Research Institute for Democracy, Society, and Emerging Technology (DSET) issued a report warning of these risks. The report traced the origins of this AI supply chain to Bitmain, a Chinese cryptocurrency mining hardware firm that had spun off its AI chip business but continued to collaborate with TSMC. According to DSET, Bitmain operated through a "remote poaching model," engaging Taiwanese chip design engineers from afar and outsourcing chip production to TSMC. Sophgo eventually emerged as a direct continuation of this AI-focused lineage.[7]

These connections were publicly traceable through open-source information, underscoring the need for more rigorous due diligence practices by Taiwanese firms. High-risk clients must be flagged and monitored through internal alert systems to prevent future breaches. Although Taiwan's Ministry of Justice Investigation Bureau successfully disrupted some of Bitmain's local partnerships, these actions were reactive and lacked the backing of a comprehensive regulatory framework. A more systematic risk management mechanism—rooted in a localized coordination framework between the Taiwanese government and domestic firms—is needed to proactively alert companies to high-risk entities like Sophgo.

This regulatory gap is part of a broader issue: Taiwan's deeper role in China's AI chip ecosystem. In December 2024, another DSET report revealed how the Shenzhen municipal government actively nurtured Huawei's shadow supply chain as part of a broader campaign for indigenous tech self-

sufficiency. Among the report's most striking findings was the involvement of several Taiwanese suppliers—though not chipmakers themselves—in supporting this shadow network. These firms provided essential services such as cleanroom construction, chemical supply, and waste management for Huawei-related production facilities.[8]

This reflects a structural and regulatory vulnerability. While the U.S. dominates chip design and equipment manufacturing, Taiwan is central to semiconductor fabrication, backed by a dense industrial ecosystem. Beyond major foundries like TSMC, United Microelectronics Corporation (UMC), and Powerchip Semiconductor Manufacturing Corporation (PSMC), hundreds of supporting firms play key roles in enabling advanced manufacturing. Although Taiwan's outbound investment screening has been relatively effective in preventing its leading foundries from transferring sensitive technologies to China, this regime does not currently extend to many adjacent suppliers. As a result, while the core of chip manufacturing remains well-regulated, many support companies have quietly entered the Chinese market, localized their operations, and become embedded in China's domestic chipmaking infrastructure.

These supporting firms fall outside both U.S. export control authority and Taiwan's existing restrictions. Yet they are actively contributing to China's goal of semiconductor self-reliance. This undermines trust between Taiwan and its democratic partners—especially the U.S.—which Taiwan views not only as a manufacturing partner, but also as a strategic ally in countering China's techno-authoritarian expansion.

## Global Impact of China's Expanding Semiconductor Capacity

While the U.S. continues to expand its export controls, it is also pursuing a broader agenda of industrial revitalization, particularly through reshoring high-end manufacturing. TSMC has become a cornerstone of this strategy. Taiwan's government has embraced the opportunity to deepen ties with the U.S., seeing its participation in this reindustrialization drive as beneficial

to the national interest. This approach was reflected in both President Lai Ching-te's recent interview with *Nikkei Asia* and Taiwan's official public comment during the U.S. Section 232 national security investigation.[9]

For Taiwan to sustain this role, it must preserve its technological edge and efficiency in semiconductor manufacturing. Yet these strengths are under threat, particularly in the mature-node segment of the industry. Unlike cutting-edge chips, legacy semiconductors are not easily restricted by export controls, as their production involves fewer U.S.-origin technologies. China has been quick to exploit this loophole by aggressively expanding its capabilities in mature-node chips, which are essential for sectors like electric vehicles, renewable energy, displays, and telecommunications.

China's strategy includes large-scale demand generation and vertical integration through what is known as the "Pseudo-IDM Model." Unlike traditional Integrated Device Manufacturers (IDMs) that consolidate design, fabrication, and packaging under a single company, this model coordinates national and local governments to support ecosystems built around select "national champions." Each champion specializes in a different supply chain segment—ranging from design and materials to final assembly—and receives extensive support in the form of subsidies, infrastructure, financing, and procurement incentives.[10]

This state-driven model allows China to mass-produce legacy chips and sell them at artificially low prices. The result is global market distortion: profit margins shrink, R&D slows, and the international supply chain becomes increasingly dependent on Chinese output. The implications are already visible. In 2024, China held 34 percent of the global legacy chip market, just behind Taiwan's 43 percent. By 2027, China is projected to reach 47 percent, surpassing Taiwan, which is expected to drop to 36 percent. The U.S. share will remain stagnant at 4 percent.[11] If this trend continues, Taiwan's leadership in legacy chip production will erode, undermining efforts by the U.S., Europe, and Japan to establish resilient, domestic semiconductor capacities. More importantly, it will deepen the democratic world's dependence on Chinese supply chains.

## Building Trust and Including Taiwan: A Solution for Global Semiconductor Security

To confront this challenge, Taiwan must go beyond safeguarding its own industry. It must work with democratic allies to actively advance the non-red supply chain initiative. This initiative aims to restructure global supply chains by reducing reliance on Chinese technologies and building greater transparency around supply chain dependencies. One core objective is to identify and gradually eliminate the use of Chinese chips in sensitive sectors such as surveillance and defense. This will require coordinated policy action, including expanding and modernizing export control regimes to counter China's efforts to build a self-sufficient, state-led technology system.

However, Taiwan cannot simply urge its allies to take action—it must lead by example. The success of the non-red supply chain depends on the trust that democratic partners place in Taiwan's regulatory and strategic alignment. This means Taiwan must undertake its own export control reforms to better align its domestic standards with those of its allies. By doing so, Taiwan will reinforce mutual trust and strengthen its position as a key contributor to allied industrial expansion, particularly in the U.S., Japan, and Europe.

By more deeply embedding its semiconductor industry into restructured, trusted supply chains, Taiwan can not only safeguard its economic future but also play a pivotal role in excluding Chinese participation from critical technologies. Taiwan's role is indispensable; yet, the road ahead is complex. Charting a practical roadmap to realize the vision of a non-red supply chain will be a defining test of Taiwan's strategic leadership in this new era of tech geopolitics.

## Endnotes

1 Thompson Chau, Cheng Ting-Fang and Lauly Li, "Taiwan's Lai urges 'non-red' supply chain to counter 'unfair' China trade," *Nikkei Asia*, May 13, 2025, https://archive.is/vqNJu.

2 Scott Livingston, "The New Challenge of Communist Corporate Governance," CSIS Briefs, January 15, 2021, https://archive.ph/u8zR5.

3 "Huawei employees worked with China military on research projects - Bloomberg," *Reuters*, June 27, 2019, https://archive.ph/yL1Oe.

4 Min-yen Chiang, Jeremy Chih-Cheng Chang, Ming-Yen Ho, Chih-Hua Tseng, Chen-An Wei, Cosette Wu and Fanny Chao, "Walking a Tightrope: Navigating Taiwan-U.S. Semiconductor Security Under Trump 2.0," *DSET*, January 21, 2025, https://archive.ph/RQE44.

5 Gregory C. Allen, "DeepSeek, Huawei, Export Controls, and the Future of the U.S.-China AI Race," CSIS, March 7, 2025, https://archive.ph/xdnt5.

6 "TSMC suspended shipments to China firm after chip found on Huawei processor," Reuters reports," *CNBC*, October 27, 2024, https://archive.ph/MUjCR.

7 Min-yen Chiang, "The Remote Poaching Model: How China's Bitmain Acquired Taiwan's Edge AI Chip Technology and Its Implications for Economic Security," *DSET*, August 27, 2024, https://archive.ph/gboXG.

8 Tsai-Yi Wang and Min-yen Chiang, "Uncovering Huawei's Shadow Network: Shenzhen Major Industry Investment Group and Taiwanese Suppliers in China's Semiconductor Strategy," *DSET*, December 18, 2024, https://archive.ph/rnIt3.

9 Bureau of Industry and Security (U.S.), "Public Comment # 71. The Government of Taiwan. Government of Taiwan," Regulation.gov, May 21, 2025, https://archive.ph/m6JWM.

10 Jeremy Chih-Cheng Chang, Hung-Ta Lin, Tsai-Yi Wang, Min-Yen Chiang, Sunny Cheung, Chen-An Wei, Yu Ning Chou, Jasper Hung and Cosette Wu, "The Great Siege: The PRC's Comprehensive Strategy to Dominate Foundational Chips," *DSET*, April 1, 2025, https://archive.ph/ZylIM.

11 林妤柔, "紅鏈逼近！中國殺價拚擴產，台灣成熟製程晶圓廠如何突圍？" [China's Chain Approaching! China Slashes Prices to Expand Production, How Can Taiwan's Mature Process Wafer Foundries Break Through?], *TechNews*, February 11, 2025, https://archive.is/EZfds.

# Conclusion: Balancing Technological Advancement and National Security in the Digital Age

*Yi-Chieh Chen and Federica Bagna*

Military and civilian technologies no longer operate in different realms. Innovations in each of these fields today merge into dual-use capabilities, leading to what is now known as the "hidden war". Taiwan's unique relationship with China further exemplifies the complexity and difficulty of differentiating between foreign malign infiltration and collaboration. The close geographical proximity and cultural and linguistic ties between Taiwan and China further complicate the innovation-security dilemma in the technological domain.

The threat of malign infiltration in academic exchanges and technological fields such as AI, semiconductor manufacturing, information security, and cybersecurity is a pressing issue. Balancing national security, innovation ecosystems, and business development in the context of cross-Strait relations is a highly complex task. The need for careful policy coordination, international cooperation, and a robust regulatory framework is urgent, given Beijing's rapid technological development and its attempts to erode Taiwan's national security through the implementation of advanced technologies.

According to Yu-chung Shen's research, cross-Strait exchanges have undergone significant changes during Xi Jinping's third term. Chinese pressure on the island has intensified beyond military and economic coercion, expanding to include more nuanced and sophisticated methods to exert control and influence across the strait. For instance, through cross-Strait exchanges in academia, science, and technology. To counter Chinese infiltration into these fields, Taipei is reinforcing its security apparatus, guided by the principles of "depoliticization" and "risk reduction." To ensure this goal is met, dif-

ferent measures are being implemented. For example, bilateral cooperation agreements between universities and research institutions must obtain governmental approval, and partnerships with specific institutions are restricted.

In addition to preventive measures in academia, attention should continue to focus on consolidating and capitalizing on Taiwan's existing technological and institutional capacities. Taiwanese resilience in the cybersecurity realm is essential to its strategic autonomy, especially amid the AI supremacy race between the U.S. and China. Shiow-Wen Wang points out that AI is at the center of the strategic competition between the two powers. Military-civil fusion initiatives are Beijing's core strategy for developing its AI capabilities. These initiatives expand into intelligence analysis, military planning systems, cognitive warfare, cyberattacks, espionage, and propaganda. However, China currently lacks the capacity to manufacture highly advanced AI chips. On one hand, this gives Taiwan leverage based on its strategic advantage in the semiconductor manufacturing industry; on the other hand, it exposes Taiwan's industry to talent poaching and industrial espionage.

Yisuo Tzeng's argument reflects Wang's point of view. Tzeng argues that Taiwan can and should rely on its technological advantage in the semiconductor industry, as it is the global hub of advanced chip manufacturing. To narrow the disparity between the two, China repeatedly attempts to exfiltrate data and engage in cyber espionage. Beijing often relies on private companies—operating as Advanced Persistent Threat groups—to outsource its malicious cyber operations. Apart from economic espionage, Beijing's cyber operations include targeting critical infrastructure at both the governmental and societal levels to erode public trust in Taipei. To counter this strategy, Taiwan has further strengthened its counterintelligence apparatus and security efforts in the technological sectors.

To achieve a comprehensive approach to securing Taiwan's national security amid a hidden technology war, Taiwan must ensure that critical industries remain resilient amid geopolitical and technological uncertainties. To achieve this and reduce dependence on Chinese influence, supply chain

diversification is critical. Due to the loose restrictions on export controls on mature chips, China's capacity for manufacturing mature chips is expected to surpass Taiwan's in 2027, with 47 percent of the global market share. This projection indicates that dependence on Chinese supply chains worldwide is likely to grow in the near future. Min-yen Chiang thus suggests that Taiwan's ultimate focus should be on reliance on non-red supply chains to build greater transparency, reduce its dependency on Chinese technologies, and leverage its own domestic competitive advantage.

Success in the technological domain means obtaining international legitimacy and global standing while acquiring greater political, military, and economic leverage over regional or global actors. Today, dual-use capabilities are a central feature of state power, with more and more technologies designed for civilian use increasingly serving strategic and defense-related purposes. One could argue that any technological advancement can be transformed into dual-use capacities—their ultimate application depends solely on the creativity and strategic foresight of the actor in question. In this geopolitical setup, Taiwan finds itself in a strategic yet vulnerable position. Standing as a forerunner and innovator in the advanced semiconductor industry and caught in complex geopolitical schemes, leveraging its competitive edge has become more vital than ever.

Technological advancements are progressing at such a pace that Taiwan must continuously update its legal frameworks, which often struggle to keep up with the evolving technological landscape. Chinese infiltration into Taiwan's technological realm represents a growing threat not only to cross-Strait relations but also to the broader global framework. Given its worldwide implications, Taiwan's national security and protection against malign infiltration are today matters of paramount urgency and concern for the international community as a whole.

This volume provides an overview of the current situation in Taiwan, raises awareness of the growing threats in the area, and offers insights into potential strategies and policy responses to mitigate these risks.