# Analysis of China's Cognitive Warfare Tactics Against Taiwan in 2025

In 2025, China conducted comprehensive cognitive warfare against Taiwan through its party, state, and military systems. In addition to mobilizing its official propaganda platforms, China adopted a government-civilian partnership model and integrated its collaborative organizations with technological measures, seeking to manipulate Taiwan's public opinion and shape an atmosphere conducive to the objective of "unifying with Taiwan."

## I. Strategic goals

In pursuit of the goal of annexing Taiwan, China has long employed a diverse range of tactics, including anonymous smear campaigns, deployment of internet water army to amplify certain narratives, manipulation through inauthentic accounts*, and the expansion of external propaganda to disseminate disinformation and steer public opinion in Taiwan. In particular, China focuses on the narratives fostering skepticism towards the US, the military, and President Lai and hypes up selected current events. In this way, China aims to achieve its strategic goals of "exacerbating internal divisions within Taiwan," "weakening Taiwanese people's will to resist the enemy," "influencing allies' willingness to support Taiwan," and "winning support for China's stance" (as shown in Figure 1).

*Inauthentic accounts refer to social media accounts not operated by genuine users. These accounts are characterized by the absence of personal life posts, no record of interpersonal interactions, misrepresentation of gender information in the account profile, or the use of foreign personas to post content in Chinese.

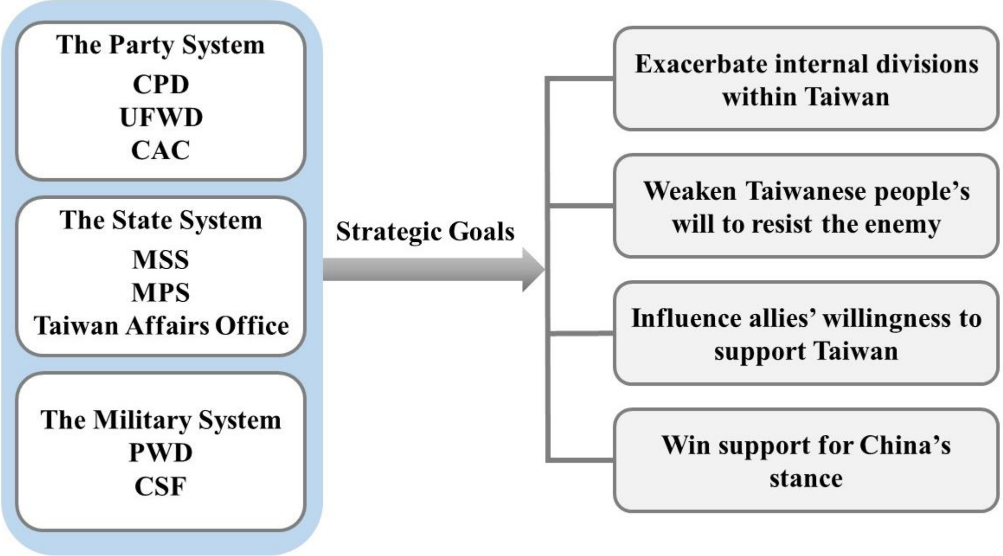
The Party System
CPD
UFWD
CAC
The State System
MSS
MPS
Taiwan Affairs Office
The Military System
PWD
CSF
Strategic Goals
Exacerbate internal divisions within Taiwan
Weaken Taiwanese people's will to resist the enemy
Influence allies' willingness to support Taiwan
Win support for China's stance

Figure 1: Strategic goals of China's cognitive warfare against Taiwan

## II. Five major tactics employed by China's collaborative organizations

China's party, state, and military systems select specific narrative themes and tones in line with the cognitive warfare objectives and then mobilize collaborative organizations, including information technology (IT) companies, marketing firms, and internet water army groups, to collect intelligence on social dynamics in Taiwan. They have employed a variety of channels, including online social media platforms and fake websites to disseminate disinformation targeting audiences in Taiwan. The five major tactics of cognitive warfare against Taiwan are applied in an integrated and flexible manner as follows (as shown in Figure 2).

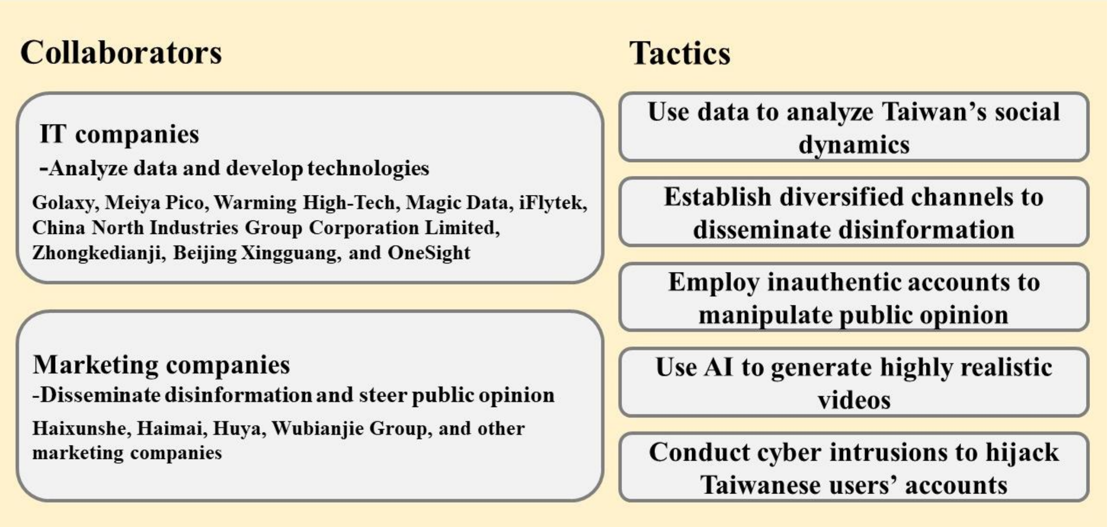
Collaborators
IT companies
-Analyze data and develop technologies
Golaxy, Meiya Pico, Warming High-Tech, Magic Data, iFlytek, China North Industries Group Corporation Limited, Zhongkedianji, Beijing Xingguang, and OneSight
Marketing companies
-Disseminate disinformation and steer public opinion
Haixunshe, Haimai, Huya, Wubianjie Group, and other marketing companies
Tactics
Use data to analyze Taiwan's social dynamics
Establish diversified channels to disseminate disinformation
Employ inauthentic accounts to manipulate public opinion
Use AI to generate highly realistic videos
Conduct cyber intrusions to hijack Taiwanese users' accounts

Figure 2: Information manipulation tactics against Taiwan employed by China's collaborators

1. Using data to analyze Taiwan's social dynamics

The Cyberspace Administration of China (CAC), Ministry of State Security (MSS), Political Work Department (PWD) under the People's Liberation Army (PLA), along with other organs, have directed Chinese IT companies such as Golaxy and Meiya Pico to utilize web crawler technology and automated data extraction programs to extensively collect online data. The data is used to build databases profiling Taiwan's political figures, legislators, and opinion leaders, including their interpersonal connections and stances toward China, so as to launch targeted propaganda campaigns toward Taiwan and attacks against specific individuals.

Additionally, during Taiwan's election periods, Chinese enterprises, such as Warming High-Tech, are tasked with compiling information on candidates' remarks, activities, polling data, and volume on social media, to assess electoral developments. They also collect information concerning social-media posts, comments, and Like counts from Taiwanese internet users to analyze public views on specific domestic, cross-strait, and international issues, so as to gauge public opinion in Taiwan's society.

2. Establishing diversified channels to disseminate disinformation: China employs a wide range of channels to spread disinformation in Taiwan, including

A. Fake websites: China's Central Publicity Department (CPD) and Ministry of Public Security (MPS) have utilized marketing companies such as Haixunshe, Haimai, and Huya to create fake websites. Those sites masquerade as neutral international media outlets, such as "Aisa Korea" and "Austria Weekly," and act in concert to spread narratives aligned with China's official stances and mislead the public.

B. Content farms and cover channels: China has supported Chinese enterprise Wubianjie Group in operating large numbers of content farms via Facebook fan pages. Their administrator accounts are mostly geolocated in Hong Kong, and tend to post sensational articles to attract clicks and traffic. Furthermore, the Wubianjie Group has also established soft-content (lifestyle/entertainment) channels on platforms such as Threads and X to build follower bases, and then pivoted to political posts, aiming to influence Taiwanese public perception.

3. Employing inauthentic accounts to manipulate public opinion

Dragonbridge, an internet water army employed by the MPS, conducts influence operations in more than 20 languages across over 180 social media platforms worldwide, such as Reddit and BlogSpot. It also establishes collaborative relationships with multiple marketing companies. Recently, it posted contents on Japan-based platform Pixiv and on platforms widely used by Taiwanese users, such as Facebook and Pixnet, to hype up disinformation claiming that "Sanae Takaichi is inciting a conflict in the Taiwan Strait," while impersonating users of differing political stances to flood those platforms with fake posts to inflame polarization and drive mutual recriminations.

In addition, units including the CAC, United Front Work Department (UFWD), and the PLA Cyberspace Force (CSF) have tasked Chinese technology companies such as Zhongkedianji, Beijing Xingguang, and OneSight with establishing netizen databases and leveraging generative artificial intelligence (AI) technologies to disseminate disinformation via automated programs managing over 10,000 bot accounts, aiming to influence targeted audiences and manipulate public opinion.

4. Using AI to generate highly realistic videos

Enterprises such as China North Industries Group Corporation Limited have developed AI models and intelligent guidance systems aiming to concurrently conduct public-opinion data collection, automated video generation, and precise delivery to targeted audiences. These systems can rapidly produce and disseminate various forms of text, audio, and video disinformation.

Moreover, China has commissioned Chinese IT companies such as Magic Data and iFlytek to develop intelligent voice systems and place advertisements on recruitment websites, aiming to entice unwitting Taiwanese users to submit online recordings in Mandarin, Taiwanese Hokkien, and Hakka. With these voice datasets, China intends to establish a database of Taiwanese accents. We do not rule out the possibility that this system can be used to clone voices mimicking Taiwanese accents, thereby enhancing the authenticity of AI-generated video content.

5. Conducting cyber intrusions to hijack Taiwanese users' accounts

During China's military exercise against Taiwan in April 2025, Chinese cyber army hijacked over a dozen PTT user accounts. Chinese threat actors also hacked into IoT devices, and rented overseas servers as proxies to hype up disinformation such as "China has blockaded Taiwan's natural-gas shipments" and "Chinese warships have entered Taiwan's 24-nautical-mile zone."

## III. Conclusion

China has integrated techniques and resources from the party, state, and military systems, as well as private companies to conduct comprehensive infiltration into Taiwan's public opinion environment. In particular, it has utilized AI technology to generate highly realistic disinformation and employed big data analysis to precisely disseminate massive disinformation, attempting to mislead the perception of Taiwanese people. In 2025, the NSB recorded over 45,000 sets of inauthentic accounts, an increase of over 17,000 sets compared to 2024. Moreover, the NSB recorded over 2.314 million pieces of disinformation the same year. Over 3,200 pieces of disinformation were reported to relevant government agencies, thereby allowing Taiwan's government to tackle China's threats of cognitive warfare in real time (as shown in Figure 3).

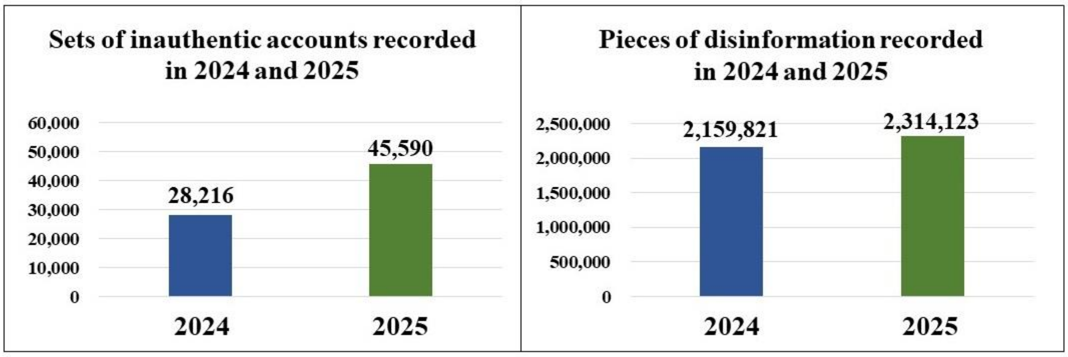

Figure 3: Numbers of inauthentic accounts and disinformation recorded in 2024 and 2025

China has expanded the targets of its cognitive warfare to include countries in the global democratic camp. In response, in 2025, government agencies and prominent think tanks in the US, EU, Australia, and France all issued reports to warn against China's manipulation of information (as shown in the Table below). This demonstrates that China's cognitive warfare threats have raised grave concerns among democratic countries. Taiwan is at the forefront of international efforts to counter China's cognitive warfare. Therefore, in 2025, the NSB engaged in over 80 security dialogues and intelligence conferences to share Taiwan's experience and techniques in combating disinformation with international friends and allies, so as to expand the cooperative network in the democratic community to counter China's cognitive warfare.

The NSB will continue to stay abreast of China's tactics of cognitive warfare against Taiwan. In addition to implementing the reporting and response mechanism across government apparatuses, the NSB will step up efforts to cooperate with third-party fact-checking organizations and social media platform operators, urging them to duly disclose and take down false information. By doing so, the NSB aims to prevent hostile foreign forces from conducting influence operations against Taiwan, thereby ensuring an unmanipulated public opinion arena in Taiwan.

| Date | Organization | Report title | Key warning content |
|---|---|---|---|
| Mar. 11, 2025 | Swedish Security Service | The Swedish Security Service 2024-2025 | China utilizes intelligence gathering and various influence operations to interfere with the decision-making processes of other countries. |
| Mar. 19, 2025 | European External Action Service (EEAS, the EU) | Third EEAS Report on FIMI Threats | China uses Dragonbridge, a Chinese cyber army group, and generative AI technology to conduct information manipulation in multiple languages, interfering with the public opinion in democratic countries. |
| Mar. 25, 2025 | Office of the Director of National Intelligence (the US) | 2025 Annual Threat Assessment of the US Intelligence Community | China expands the use of generative AI tools to enhance its global influence operations. |
| Aug. 6, 2025 | Vanderbilt University (the US) | The GoLaxy Documents | China-based Golaxy company used AI technology to generate bot accounts to interfere with Taiwan's 2024 presidential election. |
| Oct. 1, 2025 | European Network and Information Security Agency (ENISA, the EU) | ENISA Threat Landscape 2025 | China-based Zhipu AI company has created over 5,000 bot accounts on social media platforms such as X, posting extreme social commentaries and pro-China narratives. |
| Oct. 3, 2025 | Institut de Recherche Strategique de L'Ecole Militaire (IRSEM, France) | Anatomy of a Chinese Information Influence Ecosystem | China extensively utilizes fake websites to carry out political propaganda and cognitive warfare. |
| Oct.15, 2025 | Military Intelligence Section 5 (MI5, the UK) | Annual Threat Update | China employs covert and deceptive tactics to steer British public opinion and influence political decision-making. |
| Nov. 28, 2025 | Australia Strategic Policy Institute (ASPI) | Normalising Disinformation: China Shifts to Overt Operations | China uses social media accounts of its embassies and state media outlets to promote false narratives and "normalize" disinformation. |
| Dec. 1, 2025 | ASPI | AI-Enhanced Censorship and Surveillance | China utilizes generative AI and large language models to generate political propaganda in a large scale. |

Table: International government agencies and think tanks warn of China's threats of cognitive warfare