

Analysis on the Infiltration Tactics Concerning China's Espionage Cases

China has continued to employ diverse channels and tactics to infiltrate various sectors in Taiwan, recruit Taiwanese nationals to assist in developing organizations, or obtain sensitive intelligence from the Taiwanese government. To prevent China from recruiting internal co-optees in Taiwan, the national security intelligence community has implemented joint countermeasures and investigations to fully provide its support to the detection and prosecution of China's espionage cases. Additionally, China's infiltration channels and tactics in Taiwan have also been comprehensively analyzed and disclosed as follows.

I. Cases uncovered: In recent years, the number of individuals prosecuted for Chinese espionage has increased significantly, with 48 in 2023 and 64 in 2024, representing a sharp increase compared to 2021 and 2022 (see Figure 1). In addition, the number of prosecuted cases has also risen from 3 cases in 2021 and 5 cases in 2022 to 14 cases in 2023 and 15 cases in 2024. (Cases involved in Anti-Infiltration Act are not included as per above-mentioned numbers)

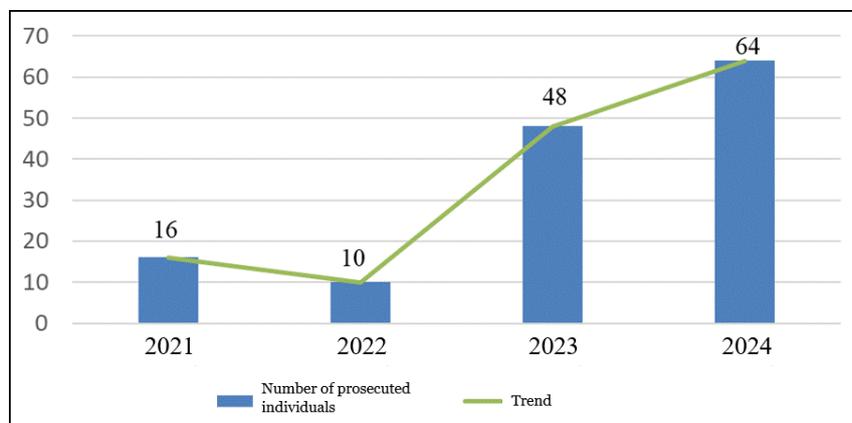


Figure 1: Statistics on the number of prosecuted Chinese spies from 2021 to 2024

II. Infiltration targets: China's main targets include military units, government agencies, and local associations, with active servicemembers and veterans making the largest proportion. In 2024, 15 veterans and 28 active servicemembers were prosecuted, accounting for 23% and 43%, respectively. This indicates that active servicemembers are China's main infiltration targets in Taiwan.

III. Five primary channels and four tactics for infiltration: Analyzing the patterns of espionage cases in 2024, it is observed there are five primary infiltration channels, such as gang groups, underground banks, front companies, temples and religious groups, as well as local associations. Also, by employing the four infiltration tactics, including using retired servicemembers to recruit active ones, establishing networks through the internet, lure of money, and coercing individuals by exploiting their debts, China conducts infiltration into Taiwan's military units, government agencies, and pro-China organizations. Such efforts aim to gain access to sensitive intelligence of Taiwan's national defense, and to develop espionage and co-optee networks in Taiwan, and even to intervene in Taiwan's democratic elections (see Figure 2).

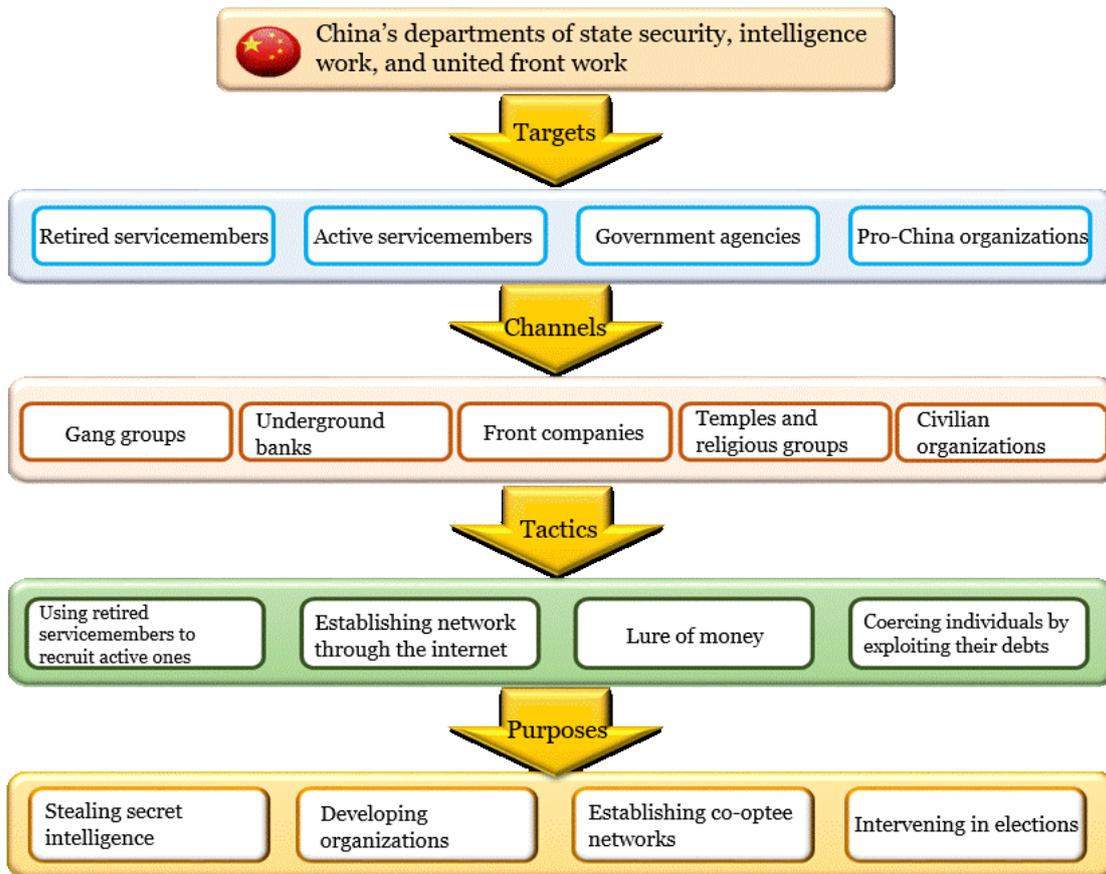


Figure 2: Five primary channels and four tactics for China's infiltration

IV. Indicative cases

1. Colluding with gang groups to develop internal armed co-optees: China has recruited members of Taiwanese gang groups, using the incentive of debt exemption to target servicemembers with financial difficulties, aiming to collect and probe sensitive government intelligence. China has also required the gang members to raise the Chinese five-star flag as a sign of internal co-optees during China's military invasion of Taiwan, in order to launch sabotage, accordingly. Meanwhile, China has utilized underground exchange channels through gang groups to bring in China's funds, instructed veterans to collect lists of high-ranking military officers, photos and coordinates of important locations such as foreign embassies in

Taiwan, military radar stations, and joint training bases. The aim is to organize those former military comrades in establishing “sniper teams” and to plan sniper missions.

2. Establishing underground banks to induce Taiwanese military servicemembers’ defection to China: China recruits retired Taiwanese servicemembers to establish shell companies as footholds, and operates underground banks and casinos, to coerce or entice active servicemembers to gather military intelligence, sign pledges to demonstrate loyalty, or pilot military helicopters to defect to China.

3. Exploiting temples to attract servicemembers to probe for secret intelligence: China provides funding to Taiwanese temples and religious groups, leveraging activities such as religious rituals for calming one’s spirits, fortune-telling, and drawing lots, to approach active servicemembers. Those individuals are coerced or enticed to film videos of defecting to China while wearing military uniforms and holding the Chinese five-star flag. They are also asked to hand over military defense planning documents.

4. Establishing united front organizations to intervene in Taiwan’s elections: China instructs Taiwan’s local associations to establish the United Front Work Committee in Taiwan. Moreover, during election periods, China organizes all-expense-paid trips for Taiwanese village chiefs and residents to visit mainland China, in exchange for their support of candidates of specific parties. Additionally, China utilizes certain online media to publish false polls and news reports, aiming to intervene in Taiwan’s elections.

5. Using the internet to establish networks and organizations:

China uses online platforms such as Facebook, LINE, and LinkedIn to offer loans to active and retired servicemembers in urgent needs of money to repay personal debts. They are asked to provide secret intelligence, recruit fellow servicemembers to expand the organization. Such maneuvers are often conducted by using cryptocurrencies to evade investigation.

V. Conclusion: In response to China's multifaceted infiltration tactics against Taiwan, national security intelligence agencies, military counterintelligence units, and judicial investigative departments have established a collaborative mechanism, constructing a common picture concerning national security threats, so as to prevent infiltration conducted by foreign forces. In addition, prosecutorial and judicial authorities have aligned their interpretations on espionage cases. This can be seen in higher rates of indictment and conviction for such offenses. In 2024, authorities dismantled a China espionage network involving 23 individuals and secured a 20-year prison sentence in a China espionage case. The successful investigation and resolution of espionage cases in recent years have also been facilitated by whistleblowing from military personnel and civilians, enabling case initiation and follow-up investigation. This indicates a significant enhancement in public awareness of counterintelligence and national security.