

In the Online Age, PRC Foreign Intelligence Evolves

Datum 3.10.2026
Subjekt Jamestown
Autor Matt Brazil
Region Zahraničie
Kategorie IT a komunikácie, Technológie, Bezpečnosť

Chinese intelligence efforts are increasingly moving away from human intelligence (HUMINT) collection to digital operations launched from within the People's Republic of China (PRC). The Ministry of State Security (MSS), military intelligence, and others have started to employ online recruiting to replace face-to-face contact for foreign assets. Beijing likely adopted the new model in response to the 2018 arrest of Xu Yanjun—the first MSS officer to be tried and convicted in the United States—which highlighted counterintelligence risks facing officers operating outside PRC borders. The MSS is using LinkedIn en masse to recruit and develop assets overseas. These operations frequently involve headhunter-style approaches and commercial pretexts to collect resumes and gather intelligence. Traditional HUMINT remains an important component of MSS tradecraft. MSS agents have started to integrate face-to-face contact in the PRC for managing their overseas contacts while their assets abroad deploy digital tools to facilitate operations.

Beijing's intelligence services are increasingly using massive, scattershot methods amenable to the use of artificial intelligence (AI) to recruit foreign sources without sending their own officers abroad. They rely largely but not exclusively on online platforms, commercial consulting arrangements, and third-country intermediaries to identify, assess, and recruit targets, all while reducing the risk of counterintelligence detection. Meanwhile, People's Republic of China (PRC) intelligence officers and agents continue to employ traditional face-to-face human intelligence (HUMINT) methods outside of the PRC when they pose a better chance of success.

Numerous cases have surfaced in the last few months that indicate the scale and breadth of these espionage efforts. On the digital side, these include the seizure by the U.S. Department of Justice (DOJ) of 13 Internet domains used to target U.S. citizens, including those with security clearances, as well as of additional domains used to target U.S. critical infrastructure (DOJ, June 10, August 26). On the HUMINT side, examples include the DOJ sentencing of a former senior adviser for the Federal Reserve Board of Governors to over three years in prison for "funneling sensitive Federal Reserve information to Chinese spies," and a former U.S. Army soldier pleading guilty to sending information on U.S. weapon systems to the PRC (DOJ, July 15, September 16; CNBC, September 30).

[1]

Beijing may have perceived an inflection point beginning in 2018 when Xu Yanjun (许岩俊), the first Ministry of State Security (MSS) officer to be extradited to the United States, was arrested (Reuters, November 21, 2022; National Security Archive, accessed October 1). With advancements among foreign counterespionage services, the PRC's intelligence services may have concluded that recruiting and handling assets are best conducted from within the PRC's borders.

Prisoner Exchanges Highlight Risk and Suggest Change

Xu Yanjun was convicted in 2021, and his operative, Ji Chaoqun (纪超群), was convicted shortly thereafter in 2022 (CNA, March 9, 2023; Guancha, Nov 28, 2024). In November 2024, however, both men were released and repatriated to the PRC, well before the end of their sentences. This was the first known instance where Beijing negotiated to recover intelligence personnel captured by the United States (Chicago Tribune, November 27, 2024; VOA Chinese, November 28, 2024)

In exchange, Beijing released two U.S. citizens convicted of “espionage” and one under a death sentence for drug trafficking. The lack of evidence from the Chinese side about these cases raises the possibility that Beijing decided to take the three individuals as hostages to trade for their nationals in the United States. **[2]** This swap was particularly notable as it marked the return of PRC intelligence personnel apprehended in the United States for the first time. **[3]**

As far as is publicly known, Beijing had previously eschewed efforts to recover its captured spies. In one prominent case, Chi Mak (陈麦), who ran a highly effective and longstanding technology theft operation in southern California for 20 years before he was apprehended, was ignored after his 2007 conviction. He died there in October 2022 at age 82 (Substack/HUMINT, November 21, 2025; Sina.com, May 1, 2007). **[4]**

Commercial Platforms Keep Intelligence Officers at Home

Since the U.S.-PRC negotiated swap, PRC intelligence techniques have emphasized technology-enabled recruitment and handling, suggesting that Beijing views prisoner swaps as a tool only to be used on rare occasions. The MSS has developed a workflow that allows officers to remain within the PRC’s borders, mitigating the risk of identification by hostile security services. As noted by the Belgian security service, the recruitment and handling of “individuals of interest” now “is often carried out in China or from China” (VSSE, January 14, 2025).

Five Eyes nation assessments covering cases across North America, Europe, and the Asia-Pacific between 2019–2026 describe a similar evolution in intelligence operations conducted by the People’s Liberation Army (PLA). Chinese services increasingly conduct spotting and assessment at industrial scale through LinkedIn and other professional networking platforms, encourage targets to undertake seemingly legitimate paid consulting work as an initial step, and employ third-country and private-sector intermediaries as operational cut-outs. In this form, they have adopted the semiconductor industry’s commercial talent-recruitment model (Five Eyes, March 6). The U.K. Security Service (MI5) has separately and specifically attributed comparable LinkedIn headhunter-style tradecraft—including two accounts identified as “Amanda Qiu” and “Shirly Shen”—to the MSS itself, indicating the online-recruitment shift spans both the civilian and military intelligence services rather than being unique to either (BBC, November 18, 2025).

The recruitment of former CIA and Defence Intelligence Agency officer Kevin Mallory in 2017 by the MSS was a precursor. Mallory, who was in financial difficulty, was approached on LinkedIn by a contact posing as a representative of the Shanghai Academy of Social Sciences—a think tank with documented ties to Chinese intelligence—and offered a paid “consulting” role. The relationship subsequently developed through in-person meetings in Shanghai rather than the United States (DOJ, May 17, 2019). Although Mallory was arrested before he could establish a long-term espionage operation, the case appears to have inspired, rather than discouraged, Beijing’s confidence in remote recruitment methods.

Security services across Europe report similar patterns. MI5 Director General Ken McCallum disclosed in 2023 that approximately 20,000 Britons had been approached through LinkedIn by Chinese recruiters, more than double the roughly 10,000 users MI5 had said were being targeted online by all foreign intelligence services and criminals two years earlier (The Guardian, October 18,

2023). The Canadian Security Intelligence Service has separately warned that Chinese intelligence services advertise employment opportunities through front companies, leading applicants to unknowingly work on behalf of a hostile intelligence service. Comparable warnings have also been issued by Germany's Federal Office for the Protection of the Constitution (BfV), the Netherlands' General Intelligence and Security Service (AIVD), and Czechia's Security Information Service (BIS) (BfV, 2020; AIVD, February 8, 2022; Euronews, September 16, 2024; CSIS Public Report, 2025). Such approaches continued this year, as demonstrated by the 2026 Kevin Zhang/Oriental Consulting operation, which reportedly netted substantial NATO and EU intelligence information (Hong Kong Free Press, March 28).

These industrial-scale approaches are particularly amenable to the deployment of artificial intelligence. AI systems can search and classify large numbers of publicly available professional profiles, identify combinations of access, expertise, foreign travel and possible financial or career vulnerability, and rank prospective targets for human review. Generative AI can then draft individualized approaches in the target's language, vary the supposed recruiter's identity and commercial pretext, and sustain preliminary conversations with many candidates simultaneously. The U.K. National Cyber Security Centre (NCSC) assesses that AI already provides a "capability uplift" in reconnaissance and social engineering, making both more effective; it also enables more convincing approaches without the linguistic mistakes that traditionally exposed foreign phishing and influence efforts (NCSC, January 24, 2024).

Human Recruiters Remain Valuable

Despite this growing reliance on online recruitment—likely enhanced by AI—traditional human intelligence operations have by no means disappeared. Instead, they complement digital approaches and are employed when they present the best chance of success.

Two recent cases show how human recruitment is fused with technology-enabled tradecraft. Singaporean academic Dickson Yeo was recruited by Chinese intelligence contacts he met while giving a talk in Beijing, then set up a fictitious political consulting firm and used LinkedIn's contact-suggestion algorithm to identify and approach potential sources almost daily; he received more than 400 resumes, roughly 90 percent from people with U.S. military or government security clearances, before he was caught (Straits Times, April 2, 2025). Estonian national Gerli Mutso travelled to the PRC for coordination with PLA intelligence officers who used the cover identity of a fictitious "Beijing Information Association"; she then returned to Europe and recruited Tarmo Kõuts, an Estonian scientist with access to NATO's Centre for Maritime Research and Experimentation, who subsequently supplied classified defense-research material to the PRC. Mutso was convicted in 2022 and sentenced to eight and a half years; Estonia's Supreme Court upheld her sentence in 2023 while partially annulling other elements of the conviction (ERR News, June 17, 2023).

Even with the shared linguistic background between the PRC and Taiwan, PRC intelligence officers follow a comparable trajectory over time. The Ministry of National Defense (MND) has noted that PRC tradecraft moved from direct in-person contact to introductions via third parties met outside Taiwan, to an increasing recent focus on online recruitment (CNA, April 22, 2025; MND, April 23, 2025). This suggests the shift toward remote, intermediary-based recruitment is a general trend rather than one confined to harder-target Western countries.

Conclusion

PRC intelligence officers increasingly direct foreign recruitment from the safety of the PRC, relying on online platforms, commercial intermediaries, and locally based facilitators to conduct much of the initial contact and relationship building that was traditionally done abroad. The result is a model

that reduces, but does not necessarily eliminate, operational exposure for Chinese intelligence personnel while allowing recruitment efforts to expand simultaneously, even exponentially, across multiple countries.

Notes

[1] Other examples include an MI5 warning that over 100 U.K.-linked academics had contributed to research projects funded by the MSS via a proxy (MI5, September 30); the arrest by Belgian authorities of both a man suspected of stealing semiconductor technology and an intern at NATO headquarters for spying for the PRC (CBC, July 29; Reuters, September 7); the arrest by Korean authorities of two PRC citizens accused of intercepting fighter jet communications and reportedly obtaining training materials from U.S. bases (Korea JoonAng Daily, September 29); the indictment of a man in Taiwan for leaking classified documents to PRC spies, and of another three former military personnel for collecting military secrets since 2020 (Taipei Times, August 18; Focus Taiwan, October 1); and the sentencing of an Australian businessman for compiling reports for PRC intelligence (ABC, September 10).

[2] Hostage taking is part and parcel of Beijing's playbook when dealing with foreign governments and institutions (China Brief, May 11, 2017; Substack/Strategic Narratives, July 31, 2025).

[3] The only other known example since the CCP's 1949 victory was a genuine spy swap in 2015 between the PRC and Taiwan. In an agreement enabled politically by the meeting that November between President Xi Jinping and Taiwan's then president Ma Ying-jeou (馬英九), the PRC released two Taiwanese military intelligence officers, Colonels Chu Kung-hsun (褚君軒) and Hsu Chang-kuo (許昌國) in exchange for a Chinese intelligence officer, Li Zhihao (李志豪) (Taiwan Ministry of National Defense, November 30, 2015; China Taiwan Net, December 1, 2015).

[4] Beijing similarly ignored Larry Wu-tai Chin (聶天鵬) and his wife. Having confessed to the FBI that he had spied for the PRC over the course of four decades, Chin allegedly committed suicide in jail before sentencing (Sohu.com, August 19, 2024). Years later, unofficial mainland sources began to laud his achievements as a "mole" inside the U.S. Intelligence Community (Red Song Network, January 26, 2018, October 27, 2025; Sina.com, April 8, 2020; Zhihu, March 26, 2024).

<https://jamestown.org/in-the-online-age-prc-foreign-intelligence-evolves>