THREAT ACTOR PROFILE

Chinese Ministry of State Security (MSS)

June 2026

BLOOMSBURY INTELLIGENCE & SECURITY INSTITUTE

Authors

Elliott Clark

SENIOR ANALYST

Nicole Pitassi

ANALYST

Sarah Jiang

ANALYST

Alexandra Bostenaru

GRAPHIC DESIGNER

Executive Summary

This report examines the role of the Ministry of State Security (MSS) in its operations against Europe and North America in the economic, military, and political sectors. We find that the MSS has substantial success in acquiring foreign technology, infiltrating political circles, and undermining critical infrastructure. With this in mind, China has successfully undermined the strategic interests of European and North American states. This is the resilience of their democracy, their economic independence, and the potency of their militaries.

At the same time, MSS activity has reduced China's strategic dependence upon the West, and increased the potency of its military. Furthermore, whilst there has been clear signs that countermeasures have been implemented, there is a concerning lack of resolve to protect against Chinese threats, particularly in Europe. States, particularly European ones, should look to strengthen their resolve against Chinese operations if they are to achieve security and protect their democracies.

Contents

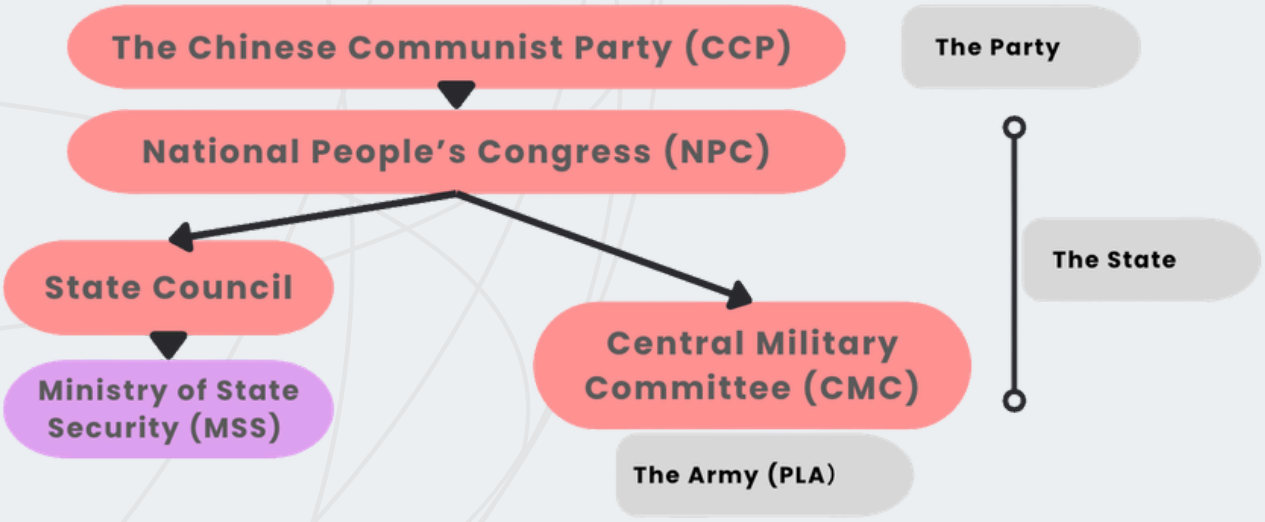
Political Objective

1. Political goals

1.1. The Party, the State, and the Army

The People's Republic of China (PRC)'s influence operations are planned, distributed, and carried out among Chinese Communist Party (CCP) members, the legislative body (the state), and the People's Liberation Army (PLA). With President Xi Jinping being the supreme leader of the 3. The internal structures of the CCP and the state organisations, including the legislative body (i.e., the National People's Congress and its standing committee), the administrative body (i.e., the State Council), and the judicial body, function within a clear hierarchical structure.

Within the CCP, departments and committees co-exist to implement Xi's doctrines. State organisations (e.g. **Ministry of State Security (MSS) of the State Council**) and the PLA of the Central Military Commission, being subordinated under the CCP, play pivotal roles in executing laws in order to ensure the sustainability of a framework (Socialism with Chinese Characteristics) that is committed to the security of the Chinese Socialist system, the authority of the CCP Central Committee with Xi being the core of that system.



Political Objective

1.2. China's strategic ambitions in the international order

China's ongoing push for economic security, restructuring of military organisation, and technological modernisation derive from Xi's goal of a "great rejuvenation of the Chinese nation". From a narrower party-state perspective, the primary national security objective lies in the security of the Chinese Socialist system and its core actors and bodies, in other words, regime security. The doctrine aligns with China's long-term strategy of integrating the ideas of modernisation and advancement into CCP doctrine whilst highlighting the supremacy of national security. Both internally and externally, national security has been maintained through the politico-legal apparatus, including the Ministry of State Security, the Ministry of Public Security, the judicial system, the Ministry of Justice, and other relevant bodies. Notably, a sustained strategic economic effort, also known as 'Fortress China', is underway to invest in research and development, manufacturing, and technology to lower reliance on Western democracies. China has been increasingly framed by Western governments and media as a 'systemic rivalry', more importantly, as a 'security threat' to the US, EU, and the UK due to its suspected espionage operations. Ultimately, the CCP aims to emerge as a global superpower and replace the existing rule-based world order with a multilateral system despite being ambiguous towards its political ambitions.

1.2.1. China's narrative-shaping efforts

Narrative 1

China is a peaceful state that is willing to pursue strategic partnerships with others for collective benefits

Narrative 2

States that against China's interests are aggressive

Narrative 3

Taiwan is part of China

Political Objective

Prior to the 2010s, Beijing had suffered a series of backlashes from the global community as a result of the 1989 Tiananmen Square Massacre and the ongoing repression of Tibetans. Therefore, Beijing's primary external strategy was to utilise its soft power, seeking to embed the idea of a friendly, pro-human-rights China and to gain international amity and discursive power. In the past decade, especially since Xi rose to power as the CCP's Premier, Beijing's external propaganda tactics have shifted towards sharp power, featuring more centralised, organised, integrated, and proactive campaigns.

Beijing seeks to project itself as a peaceful state willing to pursue strategic partnerships for collective benefit as opposed to Trump's protectionist policy. Such framing aligns with Beijing's emphasis on a "shared common destiny" among humanity, promoting coexistence and common prosperity. The idea of a shared destiny was also constantly reiterated in projects such as the Belt and Road Initiative (BRI) and strategic partnerships with Central and Eastern Europe and the Global South. Moreover, Beijing has expanded the scope of cooperation, from purely economic and infrastructure aid to a more comprehensive one that involves security cooperation and military modernisation.

A second framing of the CCP suggests that states opposed to China's interests are 'aggressive'. The narrative, despite being opaque, heavily implies the escalation of Sino-US rivalry. For instance, a state council statement describing the geopolitical norm is heading towards "junglification." The norm, dominated by hegemony and power politics, brings only warfare and insecurity. Following Venezuelan leader Maduro's arrest under US military Operation Absolute Resolve in early January this year, Trump stated the geopolitical importance of Greenland, suggesting a potential use of force to secure the island. Consequently, Trump's statement received a restrained response from Beijing, which cited the UN Charter and the violation of national sovereignty, in contrast to Trump's violation of international law.

In light of such a narrative, Japan, under the newly elected conservative Prime Minister Sanae Takaichi, was also heavily criticised by the CCP. A US-Japan alliance has always been the cornerstone of the Indo-Pacific Strategy. Even before Takaichi was sworn in, Japan had agreed to maintain the region's peace and security within the US-led alliance. Nevertheless, since Takaichi took office, Japan has been facing a drastic shift in its national defence strategy. Not only was Japan's increased defence spending rectified, but there was also a popular public sentiment to alter Japan's position on the Nuclear Principle, implying nuclear deterrence as a last resort. Consequently, these shifts in Japanese policy have provoked emotive responses from Beijing. The PLA Daily published an article condemning Japan's supposed 'neo-militarism,' suggesting that this could destabilise peace and stability in the Indo-Pacific region. This response exemplifies how the CCP's broader propaganda themes are applied to regional security developments, reinforcing Chinese perspectives through official commentary.

Political Objective

In terms of the Taiwan issue, the CCP has treated it as a domestic issue, as according to the PRC's One China Principle, "Taiwan is an inalienable part of China". The US, however, established the One China Policy, which acknowledged the One China Principle without officially recognising that "Taiwan is an inalienable part of China". The US's version of 'One China' followed the 6 assurances on arms sales to ensure peaceful cross-Strait development and engagement while legally allowing Taiwan to enhance deterrence capabilities by importing US weapons to the island. Beijing has been consolidating the One China Principle by excluding Taiwan from membership in any International organisations and would legitimise coercion if there were any official engagements with Taipei.

1.2.2. Human Intelligence (HUMINT) Capabilities

Espionage cases involved local governmental staff

Chinese espionage is one of the major tactics used by the MSS to undermine political stability, acquire military and commercial technologies, and obtain confidential information about individuals or agencies. At least 224 espionage cases have been reported in the US since 2000, with 49% of the cases directly connected to Chinese officials in the military or in the CCP. A common Chinese espionage practice in North America and Europe is to infiltrate political circles by approaching either an individual or a political party.

Such infiltration was carried out primarily through social media contacts. For instance, a recent case of Mayor Elieen Wang of the city of Arcadia was accused of being an illegal Chinese agent and was subjected to FBI investigation. Wang collaborated with Yaoning Sun in 2020 to promote CCP propaganda on Chinese diaspora communities-centric media, US News Center. Their purpose was to sway political opinions of the large Chinese-American and diaspora communities to gain discursive influence. Wang was also found to be following orders of PRC officials via WeChat to disseminate pro-Chinese articles on Xinjiang by denying forced labour and human rights violations.

Chinese espionage operations are also a modus operandi in the British and European Union parliamentary ecosystems. The EU's limited understanding of China's influence-operation structure, alongside challenges in strengthening internal resilience, resulted in major security breaches by China and other malign actors within or outside the EU.

The lack of transparency and a regulatory framework for the recruitment of Accredited Parliamentary Assistants (APAs) in the European Parliament (EP) raised concerns over exposure to malign foreign influence and the effectiveness of existing safeguards." Despite APAs handling sensitive files and confidential information when serving members of the EP (MEPs), their hiring remains informal and lacks transparency, with no standardised vetting procedure.

The EP's systemic vulnerability therefore attracts FIMI, in which unvetted APAs could leak confidential information. Alternatively, APAs could be exploited as pawns by malign actors in propaganda campaigns or intelligence operations, further fragmenting EU cohesion and its external relations. Furthermore, far-left- and right-wing political groups tend to adopt controversial narratives, often countering the EP's dominant narrative to advance their own priorities. The structural security concerns are not hypothetical, as evidenced by the arrest of Jian Guo, the APA of Alternative for Germany AfD) former MEP who was under suspicion of spying for China.

Similarly, in the UK, 2 supposed Chinese headhunters associated with the Chinese intelligence service attempted to recruit British Parliamentary staff via LinkedIn. The incident prompted MI5, the British intelligence service, to issue an espionage warning. Similar warnings have been issued in previous years, suggesting that parliamentary safeguards remain inadequate.

Espionage cases involved private actors

Among the Chinese espionage operations in Europe and North America, private actors play as important a role as official agents. The operations were commonly carried out by Chinese citizens and non-Chinese actors (i.e., non-ethnic Chinese actors recruited by the PRC) in the host countries. Operations that involve private actors tend to be associated with transnational repression, in which activists, particularly Hong Kong activists and individuals black-listed by Beijing abroad, are targeted and harassed.

In the UK, shadow policing activities have persisted since 2020. Overseas Chinese 'police service stations' were uncovered in 2023 in major cities across Britain, disguised as consultancy companies and providing overseas Chinese nationals with immigration advice and support. They often monitor local diaspora groups or even coerce some into illegal channel crossing back to China. In May this year, UK immigration officer Peter Wai and his contact, former office manager of the Hong Kong Economic and Trade Office in London, Bill Yuen were found guilty of working for Chinese intelligence. Wai abused his power and accessed the home office database to track and harass Hong Kong dissidents, with Yuen reporting the classified and personal information to Chinese authorities.

1.2.3. Technical Intelligence Capabilities

In addition to individual actors, private Chinese businesses play a role in party-state-led projects to secure official sponsorship and financial support. The competitive bidding created an unbalanced market system that incentivised the de-privatisation of business, resulting in economic stagnation due to the gradual reduction of market autonomy.

Political Objective

A recently leaked GoLaxy document evidenced the intricate relations between the central government and private corporations. GoLaxy (中科天玑) is a privately listed spin-off company, established by the Institute of Computing Technology at the Chinese Academy of Sciences (CAS). It is predominantly funded by CAS-owned companies, with the state-owned software and technology service company Dawning Information Industry Co (中科曙光) as the largest shareholder.

The GoLaxy documents exposed the operationalisation of the CCP's efforts to monitor and counter FIMI. The GoLaxy Smart Propaganda System GoPro was created to document perceptions of politically sensitive issues related to "China-US rivalry, Hong Kong, Xinjiang, and the Taiwan Strait." By integrating artificial intelligence (AI) technologies, the system was able to analyse popular emotions and stances towards targeted issues. Additionally, GoPro was able to identify key figures and organisations, either domestically-based or overseas whilst generating "immersive propaganda content" and distributing them across social media platforms. The system was even capable of simulating authentic accounts and persona as long as being fed authentic phone numbers, email addresses, and contact lists.

1.3. Effectiveness and comparison

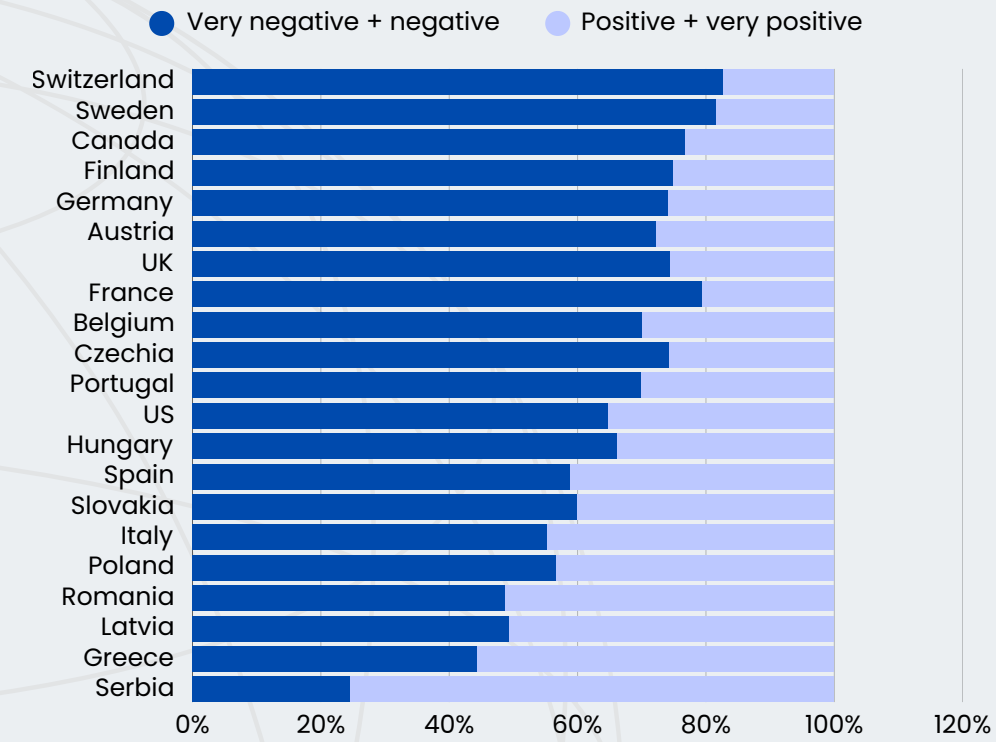
1.3.1. Asserting influence globally via rhetorical persuasion and intimidation

The CCP's attempt to legitimise its envisioned multilateral global dynamics amongst Western governments and decision-makers via propaganda slogans was only partially effective. Despite this, the targeted Western stakeholders have gradually become aware of Beijing's strategic intentions. In Europe, Beijing has shown rhetorical support for European strategic autonomy against collective protectionism, indicating a desire to remove EU-China trade barriers. However, the EU statement on the 2026 conference on EU-China relations highlighted the imbalance in trade relations between Europe and China (i.e., Chinese imports substituting for domestic products), signalling to China Europe's awareness and determination to de-risk and enhance European market resilience. Additionally, the fundamentally misaligned values between the two and China's potential involvement in the Russian-Ukrainian War prompted scepticism and caution among European nations.

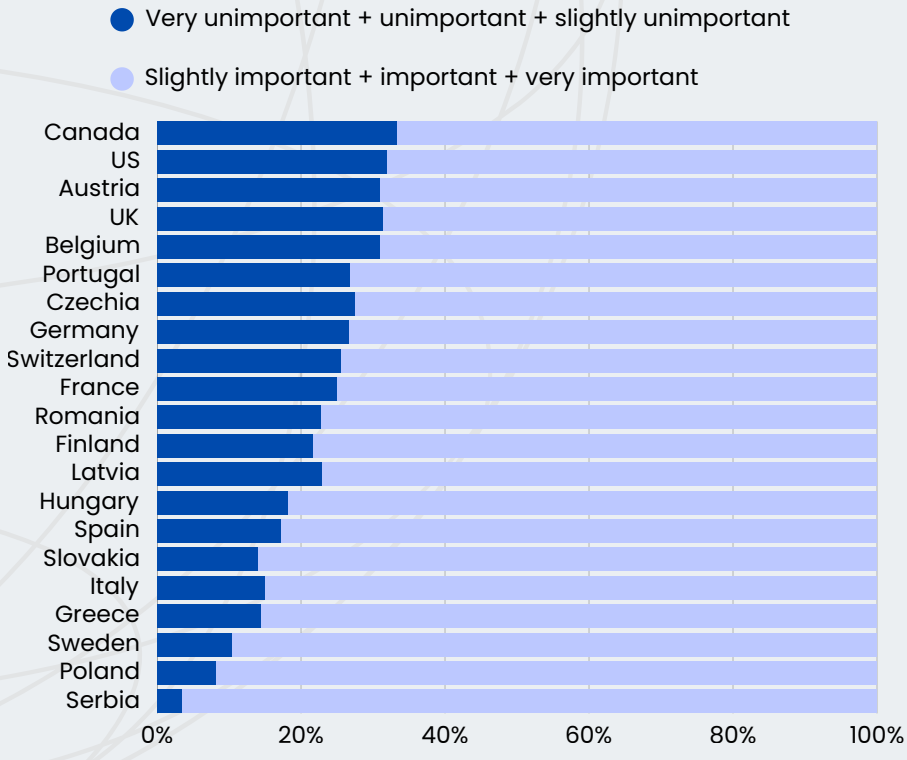
Outliers nevertheless existed, with Slovakia under Robert Fico's government exhibiting closer ties with China. The two countries have co-invested in an electric vehicle (EV) battery manufacturing project (i.e., the InoBat/Gotion High Tech battery plant) back in 2024, with another cross-brand automotive cooperation (i.e., Volvo/Geely) on the way. Such a collaboration is likely to contradict the EU's efforts to build market resilience.

Political Objective

General favourability toward China



Economic importance of China for each country's economic development



Source: CEIAS - Global Views of China Tracker

1.3.2. Infiltrating and disrupting decision-making bodies via grey-zone tactics
Human and technical intelligence operations, on the other hand, are complex and integrated yet more effective. MSS's ability to mobilise its citizens both domestically and abroad, aided by advanced technology and popular social media platforms, elevated its influence operations to a new level. Evidence suggested Chinese foreign interference during the 2021 Canadian general election. Conservative Party of Canada (CPC) leader Erin O'Toole was subjected to inaccurate reports and disinformation campaigns on Chinese-language media, potentially as a result of his motion in the Canadian House of Commons to recognise the Uyghur genocide. Meanwhile, false narratives targeted CPC British Columbia candidate Kenny Chiu over his proposal to establish a foreign influence registry. It was also shown that during elections, public opinion can be easily manipulated by the circulation of false information. New Democratic Party (NDP) MP Jenny Kwan, a candidate in the Vancouver East electoral contest, had lost popularity and approval amongst Chinese communities in her constituency due to her strong public advocacy regarding Taiwan, Hong Kong, and Uyghur issues. Despite heavy suspicion, an official statement, accompanied by cross-examined evidence, was released only two years later, in 2023, confirming the PRC's involvement in the 2021 election.

1.4. Counter measures

1.4.1. Legislative awareness and a whole-of-government approach in the US
The U.S. has adopted a whole-of-government approach in countering FIMI. For instance, the FBI initiated the National Counterintelligence Task Force (NCITF) in 2019, encouraging collaborative efforts among federal, state, and local partners, as well as non-traditional partners such as civil society agencies. Additionally, the US government continues to bridge the information gap by releasing annual official publications that provide comprehensive updates concerning US-China relations, China's domestic development and policies analysis, defence and technological spending, PLA force employment, and politically sensitive issues.

Foreign Agent Registration Act (FARA) and baby FARAs
Building upon these governmental measures, the Foreign Agents Registration Act (FARA), originally enacted in 1938, and Title 18 of the United States (Federal Criminal) Code, Section 951, are the fundamental legal mechanisms for countering FIMI in the US. Under FARA, any agent or entity of a foreign government that engages in political activities must register with the US Department of Justice (DOJ) and periodically disclose its activities to the public. Nevertheless, FARA was considered an 'obscure law' until major foreign election interference in 2016, when it was actively enforced by the DOJ through increased audits, civil settlements, and criminal prosecutions. The frequency of FARA enforcement raised serious questions about overly aggressive interpretations of the act and about potential human rights violations.

Political Objective

Starting in 2024, the decentralisation efforts to counter foreign influence began with predominantly Republican states adopting bills similar to FARA, commonly called 'baby FARAs. Arizona, California, Georgia, Oklahoma, and Tennessee were the first states to adopt baby FARAs, following Texas, Louisiana, Nebraska, Arkansas, and Florida in 2025. Notably, baby FARAs vary from the federal statute amongst states, with some states only targeting countries such as China, Russia, North Korea, Iran, and the Maduro regime in Venezuela. As the adoption of baby FARAs is in its early stages, issues such as exemptions for commercial entities arise and require more detailed legal interpretation.

1.4.2. Caretaker Convention in Canada

The caretaker convention is a mechanism designed to ensure proper representation of public opinion during election periods or when the incumbent government is dissolved. During this period, all government activities must be limited to official governmental duties (e.g., international treaty negotiations). Moreover, members of parliament should distinguish between official business and partisan political activities, ensuring that financial and human resources are not used for partisan purposes. It is also required that the ministers conduct official business in a low-profile manner. While the caretaker convention is not a legal mechanism specifically targeting foreign election interference, such practice could sustainably minimise the risks of any malign interference during the election period.

In the case of the UK, similar rules applied to the pre-election (purdah) period and post-election caretaker period. Governmental due diligence efforts have been intensified, focusing heavily on political financing regulations, enhancing penalisation, and ensuring the resilience of information systems. Nevertheless, the political will to optimise the existing caretaker convention has been absent in the UK.

1.4.3. China Watchers and think tank efforts in Europe

Due to Beijing's increasing influence on the other side of the Eurasian continent, not only governmental initiatives but also non-governmental actors began taking steps to de-risk against both Chinese influence operations and its strategic economic policies. Robust China-watching groups have sprouted globally, such as the China Observer in Central and Eastern Europe (CHOICE) and Young China Watchers (YCW), a global network that hosts cultural activities, forums, and dialogues on all aspects of China. In addition, several think tanks branched out with departments specifically dedicated to research on Asia and China. For instance, the Mercator Institute for China Studies (MERICS), the Institute of International and Strategic Studies China Programme (IISS), or Chatham House China-focused analysis.

Political Objective

The Central European Institute of Asian Studies (CEIAS), a think tank based in Slovakia that focuses on Europe-Asia relations, has initiated multiple projects to update and track developments on China-related issues. In terms of academic security, an academic engagement tracker was established to highlight potential bilateral links and areas of cooperation, including AI, quantum computing, semiconductors, materials research, aerospace, robotics, and electric vehicles.

1.4.4. Deliberative democracy

Existing countermeasures against influence operations remain fragmented and regionally isolated. Given the CCP and MSS's worldwide network and the escalation of grey-zone intelligence activity, there is now an urgent need for an integrated transnational counter-FIMI and intelligence-sharing platform, explicitly rooted in deliberative democracy. Such a platform must enable intelligence sharing among states and actively engage civil society and citizen assemblies to pool collective vigilance and resilience.

The FIVE EYES alliance (the US, the UK, Canada, Australia, and New Zealand) is an initiative that comprises the fundamental elements of a platform. Nevertheless, to address non-traditional espionage agents, the scope and membership of such an alliance should be expanded to include allies in the Indo-Pacific region. Taiwan, in particular, should be considered a potential partner in such a framework, given the island's extensive experience in responding to Chinese FIMI activities. The collective efforts of government agencies, civil society, and independent fact-checking initiatives have contributed immensely to both debunking and pre-bunking disinformation campaigns. A relevant example followed Chinese state media's criticism of Japan's perceived return to 'militarism'; the Taiwan Information Environment Research Centre (IORG) quickly identified the narrative as part of a broader information operation and warned Taiwanese audiences not to respond to the false claims. Beyond governmental efforts, civil society and the private sector also played pivotal roles on the island. DPP legislator and activist Puma Shen founded the Kuma Academy that offers online and in-person training courses to improve citizens' media literacy and awareness of FIMI. In integrating emerging technology into deterrence capabilities, the private sector provided the government with practical suggestions on the stages of development and, on the government's behalf, secured partnerships and collaboration opportunities with like-minded allies in the same industry. Whole-of-society resilience is strengthened through sustainable cooperation amongst state institutions, civil society, public and private initiatives, and, most importantly, informed citizens. Taiwan's countermeasures could therefore inform the development of a broader transnational alliance, capable of countering FIMI while strengthening democratic resilience.

Major Operations

2023 -2026

- Illegal Chinese overseas police stations

2026

- Arcadia city mayor Eileen Wang found guilty for Chinese espionage

2025

- CCP-aligned firm GoLaxy leaked documents that revealed the operationalisation behind AI-driven propaganda

Canada

2019-2021

- Chinese interference found during the 2021 Canadian general election

United Kingdom

2026

- The new Chinese embassy in London was under suspicion of being a 'Chinese spy hub'
- Illegal Chinese civilian police harassing Hong Kong dissidents

2025

- Jiaotong-Liverpool University came under security scrutiny due to linkage to Chinese and Russian blacklisted entities

European Union

2023-2025

- Baltic-Sea Internet cables sabotaged by Chinese-operated carriers

2024

- German far-right party (AfD) member's assistant Jian Guo arrested for spying for Chinese security apparatus

Major Operations

2016–2023

- US/Europe: Aquatic Panda (which operates under the APT41 umbrella) conducted multiple espionage campaigns. In 2025, the US Department of Justice (DOJ) charged 12 employees for their involvement across this period.

2022–2024

US (Schultz case): Former US Army intelligence analyst Korbein Schultz collected and transmitted 92 classified documents to an individual believed to be affiliated with the PRC, in exchange for approximately USD 42,000. Material transmitted included:

- His unit's operational order before its deployment to Eastern Europe in support of NATO operations.
- US Army lessons learned from the Ukraine/Russia conflict, applicable to Taiwan's defense
- Technical manuals for the HH-60 helicopter, F-22A fighter aircraft, and ICBM systems.
- Information on Chinese military tactics and the PLA Rocket Force.
- Details on US military exercises in South Korea and the Philippines.
- Documents on US military satellites and missile defense systems (HIMARS, THAAD).
- Tactics for countering UAVs in large-scale combat operations.
- US Navy operational security and military training information.
- Details on a ground and air-based radar system located in Japan.

2024

- US: Two active-duty US Army soldiers were charged with obtaining and transmitting national defense information to individuals in China, including secret and top-secret hard drives, information on US military weapon systems, and information on US military readiness in the event of a conflict with China.

January–March 2024

- US: Salt Typhoon exfiltrated configuration files from US government and critical infrastructure entities, including two US state government agencies. The group compromised a state's National Guard system.

Major Operations

June 2024

- US: UNC3886 targeted a US-based aerospace manufacturer, exploiting zero-day and high-impact vulnerabilities in network and virtualisation devices.

September 2024

- US: The US government disrupted a Flax Typhoon botnet. Azurite, operating under the Flax Typhoon umbrella, continued gaining long-term access to OT engineering workstations across manufacturing, defense, utilities, and alarm systems in the US, Europe, and Asia-Pacific.

September 2024-2025

- US: Salt Typhoon breached major US telecom carriers (confirmed: AT&T, Verizon, CenturyLink, Charter Communications, Windstream, and Consolidated Communications). The operation compromised the lawful wiretapping systems used by US intelligence and law enforcement. Phone conversations of President Donald Trump and Vice President Vance are among those affected.

November 2024-August 2025

- Germany: Martin D., a former US defense contractor, was arrested in Frankfurt Airport after offering sensitive US military information to Chinese intelligence services multiple times during the summer of 2024. German federal prosecutors indicted him in August 2025.

2025

- US and French authorities tried to clean thousands of computers infected with PlugX RAT by Mustang Panda.

January 2025

- US: Silk Typhoon exploited a zero-day vulnerability in the Ivanti Pulse Connect VPN to switch from on-premises environments to cloud environments, dumping Active Directory data and stealing passwords.
- US: The Department of the Treasury sanctioned Salt Typhoon front company Sichuan Juxinhe Network Technology Co., Ltd.

Major Operations

February 2025

- US: A post appeared on Craigslist advertising “Job Opportunities for recently laid-off US government employees”. The link led to a consulting company in Singapore, which was part of a broader MSS-connected network of websites, LinkedIn pages, and job advertisements targeting former government employees.

March 2025

- US: Microsoft reported that Silk Typhoon was targeting widely used IT management tools and service providers, stealing API keys and credentials to gain downstream access to client networks.
- US: DOJ charged 12 Chinese nationals, including two Ministry of Public Security (MPS) officers and employees of i-Soon (APT27), for global computer intrusion campaigns targeting US defense contractors, think tanks, government agencies, and universities. Stolen data was brokered to MSS and MPS.
- US: DOJ indicted Yin Kecheng and Zhou Shuai (part of Sil Typhoon) for hacking the US critical infrastructure and the Treasury Department, with data collected under MSS-supplied targeting parameters.

2002-April 2025

- Germany: Jian Guo, a leading member of the AfD party, began passing confidential documents to Chinese authorities via a handler working for a logistics company at Leipzig airport (key hub for the German defense industry). The handler provided data on cargo, flights, and passengers. The former AfD member was charged in September 2025.

May 2025

- Czech Republic: The Ministry of Foreign Affairs was targeted by a Chinese cyberattack campaign (attributed to APT31).
- US: Salt Typhoon expanded its operations into space-related networks, compromising the Viasat satellite group's infrastructure and systems used by the US military as crisis communications backups.

June-July 2025

- US: Yuance Chen and Liren Lai were arrested and charged with MSS-directed intelligence taskings: gathering intelligence on US Navy bases and personnel, facilitating dead-drop cash payments for national security information, and recruiting military insiders. Chen had been photographed on the USS Abraham Lincoln in January 2025; he met MSS officers in Guangzhou in March 2025.

Major Operations

July 2025

- Italy-US: Xu Zewei (part of Silk Typhoon), who was directed by the MSS Shanghai State Security bureau, was arrested in Milan and faced extradition to the US.

August 2025

- Global: FBI confirmed that Salt Typhoon targeted over 80 countries and notified more than 600 organisations. Targeting was confirmed across telecom, government, transportation, and military infrastructure networks.

January 2026

- US: The US government and policy organisations were targeted by Mustang Panda using Venezuela-themed spear phishing emails.
- France: Four individuals, including two Chinese nationals, were charged with intercepting sensitive military communications. A satellite dish was installed and connected to a system of computers that recorded satellite data. Discovery coincided with a local internet outage on 30th January.

2023-February 2026

- US: A former US Air Force officer and F-35 Lightning II instructor pilot, who previously commanded units responsible for nuclear weapons delivery and flew F-4, F-15, F-16, A-10, and F-35, provided unauthorised defense services (including training) to Chinese military pilots. He passed information to a Chinese national who, in 2016, had already pleaded guilty to hacking US defense contractors. He was Charged in February 2026.

February 2026

- Greece: Air Force Colone Christos Flessas was arrested while preparing to transmit a new batch of classified information to China. He commanded a telecommunications and electronic systems training squadron with access to classified material from multiple NATO allies. He was supplied by the MSS with a specialist device to photograph and transmit documents.

Military & Technology Operations

Monitoring Western Military Capabilities and Vulnerabilities

The MSS directs efforts to acquire foreign technologies and intellectual properties illicitly to fuel China's strategic and economic ambitions through the direction of several Advanced Persistent Threat (APT) groups. The APT groups are state-linked cyber units that conduct long-term covert intrusion campaigns against foreign governments, industries, and militaries; major and more known Chinese-backed APT groups are APT41, which focuses on espionage with financially motivated operations, APT31, which targets governments and political actors, and the Typhoon cluster of groups (Salt, Volt, Flax, and Silk Typhoon), which specialise in infiltrating critical infrastructures, like IT management tools, service providers, lawful wiretapping systems, and Satellite infrastructure. By using these APT groups, the MSS aims to embed itself within the infrastructure networks that Western countries rely on, enabling China to anticipate and disrupt Western military support for Taiwan in the event of an invasion.

The use of APT groups also shows a deliberate fragmentation of the MSS structure, in which the latter contracts with private companies to conduct intrusions and steal data for sale. This allows the MSS to maintain plausible deniability, making prosecution harder, and scales operations beyond what state bureaus can achieve on their own. The deliberate fragmentation of MSS is very similar to that of the General Staff of the Russian Armed Forces (GRU), which shifted toward a greater reliance on disposable agents after 2022. GRU distributes tasks on a freelance basis, which is structurally similar to the MSS contracting private firms to conduct intrusions and broker stolen data, thereby making the prosecution of these actors harder. Moreover, both services use this fragmentation to scale operations.

Overall, Chinese military espionage targets the technological gaps it needs to close to achieve PLA modernisation goals, i.e., recruiting individuals working in the Navy, with a focus on US blue-water naval capabilities that China would need to determine its dominance in the South China Sea. Therefore, Chinese operations are not aimed at destabilising and degrading the adversary's morale or disrupting political cohesion, but rather at the long–term goal of improving Chinese military capabilities.
Chinese espionage operations in Europe, instead, are shown not to be targeting individual countries, but rather, they are trying to get access to NATO classified information, as the Greece and France cases demonstrate

Military & Technology Operations

Effectiveness of Operations

Chinese espionage operations have proven largely effective in advancing the PLA's modernisation goals, with a consistent record of using stolen intelligence to enhance military capabilities, though effectiveness varies across sectors, and Western countries are increasing the impact of their countermeasures.

China's clearest operational success is in aviation. The F-35 case involved the theft of radar schematics, engine cooling designs, and coating specifications, and in 2024, China presented the J-35A, a fighter jet built to challenge the F-35. Through the Schultz case, China acquired F-22A technical manuals, ICBM system documents, and US Army lessons learned from the Ukraine conflict that would be applicable in a potential conflict with Taiwan. Over 2 decades of operations, documents on aviation, submarine technology, space systems, and advanced electronics have been acquired, and they all map directly onto PLA modernisation goals and sectors in which China has made rapid progress.

China's operations targeting the US defence industrial base (DIB), however, have been comparatively less successful. Since the Cloud Hopper campaign exposed the managed service provider route of attack, Western export controls and supply chain screening have been improved, reducing China's ability to penetrate this sector.

The Typhoon campaigns achieved and maintained persistent access to US critical infrastructure without being detected. Specifically, they infiltrated major US telecommunications providers and gained access to the surveillance systems used by US law enforcement and intelligence agencies, as well as the satellite communications networks used by the military as crisis backups. The US government openly acknowledged in its assessments that these intrusions are extremely hard to detect because they do not use custom malware but instead rely on local network tools. The scale is also significant since there were more than 72m China-origin attack attempts against telecommunications systems between August 2023 and August 2025. However, none of these groups has disrupted a single utility, as using the pre-positioned access would constitute an act of war that would expand, rather than limit, Western involvement in a Taiwan conflict. Therefore, the current situation creates an incongruity between the extensive capabilities and their value, depending on Western decision-makers' actions toward Taiwan.

Despite the proven effectiveness of these operations, APT campaigns are increasingly gaining attention as they have been publicly attributed, sanctioned, and in some cases, disrupted. Furthermore, the American Air Force is actively building monitoring arrangements with utilities at strategic locations to improve detection of these groups, thereby undermining their effectiveness. Regarding improving the detection of operations, Western forces are becoming better acquainted and, therefore, better at detecting Chinese HUMINT operations.

Military & Technology Operations

China relies on an extensive number of sources simultaneously and accepts a certain level of detection rates as an operational cost. However, these detection rates help Western forces create demographic profiles and gain knowledge of Chinese recruitment methods, which, overall, lead to improved detection. The detection effectiveness, however, is lower in European countries, and prosecuting Chinese spies is harder, as the cases from Greece, France, and Germany demonstrate. European military establishments might offer lower intelligence value due to having less cutting-edge defense technology, but it is still valuable as they offer access to NATO military capabilities.

Europe would likely be strongly affected if a conflict initiated by China happened, given its deep economic ties to both Taiwan and China. In 2024, Taiwan was the EU's 13th largest trade partner, with €71.9b in goods trade, but the most strategically significant aspect of this relationship is semiconductor production. The COVID-19 pandemic exposed Europe's structural dependence on Taiwanese chip imports, as supply chain disruptions stretched across the automotive, electronics, and defence industries. In response, after the pandemic, Europe has strengthened its bilateral relations with Taiwan, and in 2024, TSMC opened a semiconductor fabrication plant in Germany, in a joint venture with Bosch, Infineon, and NXP, backed by a €5b European Commission support measure. In 2025, TSMC also partnered with the Technical University of Munich to establish an AI-chip R&D unit in Bavaria, which aimed at integrating Taiwanese semiconductor capabilities into Europe's critical supply chain resilience strategy.

Europe's exposure is compounded by its coexisting dependence on China, which is the EU's third-largest export partner and largest import partner. A conflict would therefore create a binary shock: the loss of Taiwanese semiconductor supply and the severing of Chinese-centred trade and green technology supply chains, on which Europe relies for over 95% of its solar panels and 90% of its permanent magnets used in electric vehicles and wind turbines.

The Russia-Ukraine war offers a reference point for scale. Between 2022 and 2023, European countries closest to the conflict lost between 1.4 and 1.8 percentage points of annual GDP growth, while eurozone inflation rose from 2.6% in 2021 to 8.4% in 2022, with energy and food inflation accounting for more than two-thirds of the increase. The total estimated cost of the war in Ukraine to affected countries is close to USD 2.4t as of July 2025. A Taiwan conflict is estimated to be significantly more damaging: Bloomberg Economics estimates that its total cost is around USD 10t, which is roughly 10% of global GDP, surpassing the combined economic blow of the Ukraine war, the COVID-19 pandemic, and the 2008 global financial crisis. Modelled first-year GDP impacts include a 40% contraction in Taiwan, 16.7% in China, and 6.7% in the United States.

Military & Technology Operations

Securing Advantage in Southeast Asia Using Western Technology

Chinese espionage has produced measurable military advantages in the Indo-Pacific, and its capability development has been accelerated by the stealth of Western technology, which would otherwise have taken decades to achieve organically.

During the F-35 case, MSS acquired information, including mission systems blueprints, from Boeing Company networks. Analysts observed that this information has been used to design the J-35's external configuration, which features diverterless supersonic inlets, a stealthy airframe, an internal weapons bay, and radar-absorbing features derived from American technology. With these technologies, Chinese pilots would be able to fly undetected until within lethal missile range, giving China a decisive first–strike advantage in any potential conflict. The West retains a comparable stealth capability through the F-35 and the F-22A; however, Western countries are concerned that China is closing the gap that has, until now, given the West a decisive first-strike advantage.

Furthermore, PLA doctrine places the Fujian carrier, one of China's most advanced aircraft carriers, with J-35A and J-15T fighters east of Taiwan, which cuts off escape routes and imposes sea and air control that would block or delay US or Japanese intervention. From the Fujian carrier, the J-35A would be able to project airpower across the entire Spratly archipelago (a contested area in the South China Sea). The general presence of J-35A in the South China Sea would extend China's anti-access/area-denial (A2/AD), which consists of a system of missiles, aircraft, and sensors that are designed to deny enemy forces entry into a defined operational zone, by over 1,000 kilometers. This directly threatens US carrier strike groups that operate from Guam, Okinawa, and the Philippines, which previously could operate from a safe standoff distance; now they are at risk of detection and engagement far earlier than in the Taiwan Strait, altering intervention calculations.

The Schultz case, which provided access to US Army lessons, led China to prepare for a prolonged, high-intensity military campaign focused on information warfare, joint-force integration, and sustained logistics. The Analysis of US military planning during the Ukraine-Russia conflict also allowed China to refine its drone-swarm tactics and PLA doctrine, which now emphasise saturating Taiwan's defences with large volumes of drones and missile salvos aimed at exhausting interceptors, combined with cyber and electronic warfare to target command-and-control and sensor-shooter connections.

Military & Technology Operations

Military & Technology Operations

At the broader strategic level, the US DoD 2025 Report assessed that China holds the world's leading hypersonic missile arsenal, including land-attack and anti-ship variants and longer-range ballistic missiles, while the US Army and Navy hypersonic programs recently passed from the prototyping phase to production, after USD 2.7b was awarded to accelerate the program completion. Furthermore, the Pentagon assessed that China's counterspace capabilities include kinetic, electronic, cyber, and directed-energy options capable of disrupting or damaging satellites. China's Guowang broadband constellation has enabled PLA missile units to find, track, and strike moving naval or land targets much faster across the Indo-Pacific. For the US, these developments increase the urgency of programs like Next Generation Air Dominance (NGAD), which aims to develop a sixth-generation air-superiority fighter to replace the F-22A and maintain US dominance in contested airspace.

Reducing Strategic Economic Dependency on the West

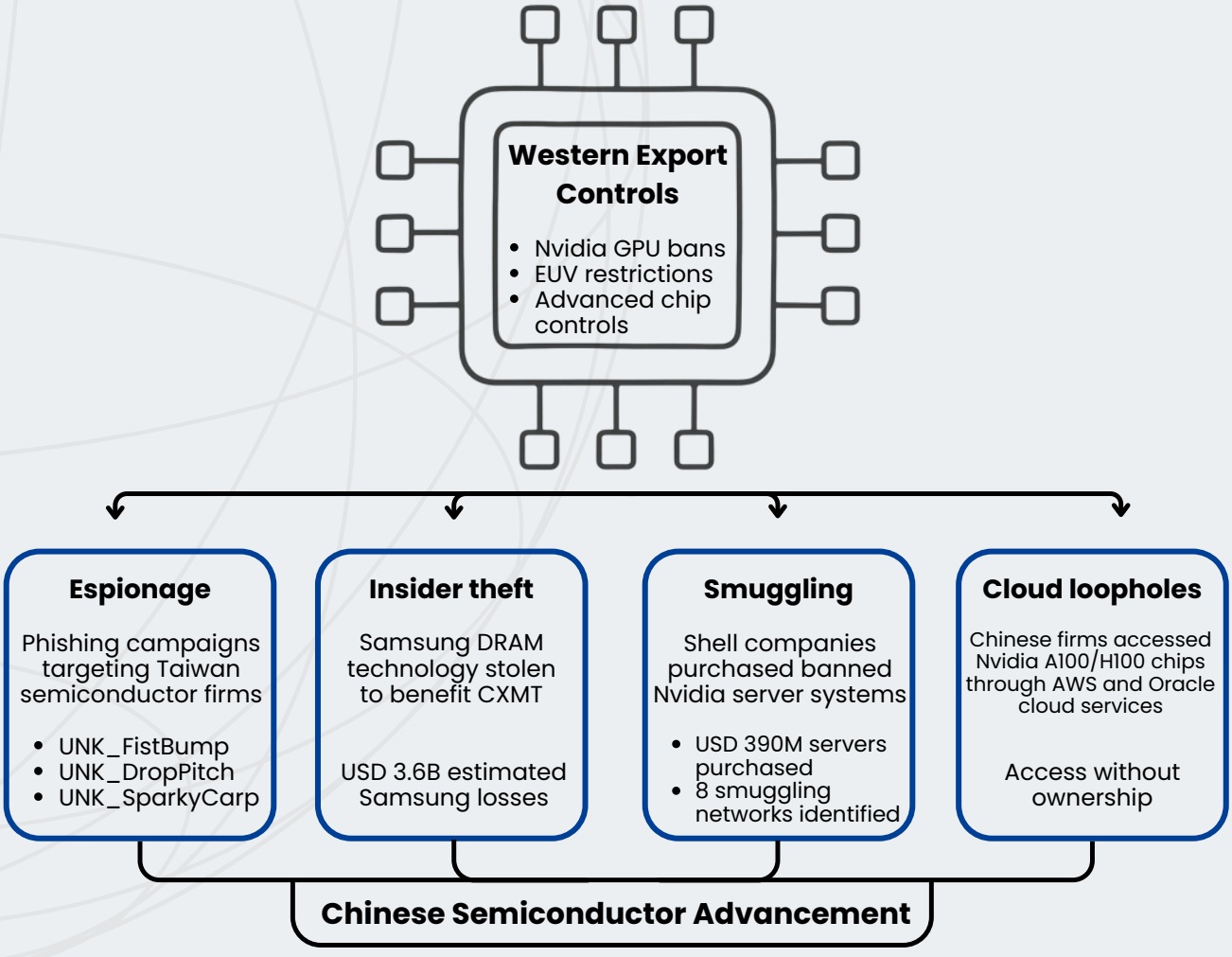
The US and its allies have imposed and tightened controls on exports of semiconductor technology to China, banning the most advanced DUV lithography tools, in an effort to maintain US leadership in the sector. This led to the creation of a semiconductor gap, which has become the clearest vulnerability, as the US and its allies dominate more than 90% of global lithography manufacturing, leaving China heavily reliant on foreign sources for chips. The main chokepoint is extreme ultraviolet lithography machines, which are used to print nanoscopic circuits on advanced microchips for the AI, smartphone, and supercomputer sectors. To counterbalance this export dependency, China relied on espionage, smuggling, and insider theft. For instance, between March and June 2025, three China-backed threat actors (tracked as UNK_FistBump, UNK_DropPitch, UNK_SparkyCarp) conducted targeted phishing campaigns against the Taiwanese semiconductor industry. Specifically, UNK_FistBump targeted semiconductor manufacturing, packaging, testing, and supply chain organisations; UNK_DropPitch targeted individuals at major investment firms who specialise in investment analysis in the Taiwanese semiconductor and technology industries; UNK_SparkyCarp conducted phishing activity against the Taiwanese Semiconductor Company.

Another example of Chinese espionage is a systematic theft of national semiconductor technology (the blueprint for Samsung's 10nm-class DRAM process), organised by 10 individuals, to benefit China's ChangXin Memory Technologies (CXMT). The breach was estimated to have cost Samsung Electronics 5t won (USD 3.6b) in lost revenue for 2024, compounded with KRW 1.6t (USD 1.2b) invested over five years to create the technology; the stolen information allowed the Chinese company to focus toward High-Bandwidth Memory (HBM), used for AI processors, and launch in November 2025 DDR5 and LPDDR5X produces which are a direct challenge to the South Korean dominance.

Military & Technology Operations

The tightening of export controls has led China to adopt a more aggressive approach to acquiring foreign semiconductor technologies. For instance, in 2024, a Chinese shell company bought USD 2.5b worth of servers from Dell and Supermicro, which contained banned Nvidia GPUs, which were reported to be traded in a Shenzhen market afterward. Eight Chinese AI chip-smuggling networks have been identified, and each engaged in transactions that were valued at more than USD 100m. Nvidia reported that revenue from Singapore rose from USD 562m in Q3 2022 to USD 2.7b in Q3 2023 alone, which could signal smuggling activity due to Singapore's limited electrical generation capacity.
To bypass the Western bans, Chinese companies have also discovered and exploited a loophole in cloud platforms like Amazon Web Services and Oracle Cloud, which allow them to use cutting-edge chips like Nvidia's A100 and H100GPUs without physically owning them.

Overall, China's efforts to gain semiconductor self-sufficiency are offsetting Western efforts to block it, as China's semiconductor self-sufficiency rate in 2024 was around 33%, and in 2025 was estimated to be around 50%, with SMIC producing 7nm chips for Huawei's Kirin processors and CXMT mass-producing DDR5 and PLDDR5 memory.



Military & Technology Operations

EU dependencies on Chinese-manufactured critical medications

Pharmaceutical security has risen in importance alongside excessive reliance on Chinese supplies of critical minerals, becoming a new security challenge in Europe and the US. During the COVID-19 pandemic, significant disruptions occurred in the global supply of essential medications due to high domestic demand in China, highlighting Beijing's dominance in the global pharmaceutical supply chain.

China, the US's largest foreign supplier of critical pharmaceutical inputs (CPIs) (e.g., raw materials, chemical compounds, and components used to manufacture medications), controls ¾ of imported CPIs. Notably, the active pharmaceutical ingredients for a specific type of antibiotics that treat common chronic diseases and HIV are predominantly sourced from China. In Europe, a stress test was conducted in the Pharmaceutical industry to determine whether the European critical medicine supply is at risk. It revealed a positive result similar to that of the US, with Chinese-supplied generic non-patent drugs accounting for 80% of the EU medicine supply. Germany's dependency on Chinese-supplied antibiotics is particularly imbalanced. For instance, there has been a gradual decline in domestic penicillin manufacturing since the 2000s due to government-imposed price caps on generic drugs, which, in turn, have led to Germany's overreliance on imported drugs.

China's emergence as a leading biopharmaceutical supplier was the result of a deliberate strategy by Beijing. The 'Made in China 2025' initiative illustrated the party-state's goal of moving beyond mass production into high-end drug development, aiming to create patented medicines that meet the standards of the International Council for Harmonisation of Technical Requirements for Pharmaceuticals for Human Use (ICH). Beijing advanced this plan by prioritising domestic pharma producers in public procurement, effectively requiring foreign companies to establish joint ventures with Chinese firms to manufacture locally.

Despite Beijing's inaction in weaponising the pharmaceutical supply chain for economic coercion, the US and EU are aware of their dependencies and are extremely cautious. It is noted that pharma trade relations between the US and China are not bilateral but instead go through third-country producers, such as European countries. Therefore, a description in the European market could indirectly impact the US market. Earlier this month, the EU announced a Critical Medicines Act (CMA) that aims to diversify the sources of medicine supplies. The CMA pinpointed several constructive pieces of advice, including modernising medicine manufacturing capacity via faster access to EU funds and support. As well as collaborative procurement. To minimise impact on the supply chain, each member state must assess broader European pharmaceutical circumstances before stockpiling for contingencies.

Military & Technology Operations

The current countermeasures put into action by the US concern investments, as from January 2025, the “Outbound Investment Security Programme” came into effect and imposes notification and restriction requirements on US persons that engage in transactions with Chinese entities in the semiconductors, quantum, information technologies, and AI sectors. The setback for this countermeasure is that the Committee on Foreign Investment in the United States (CFIUS) has not established a case-by-case review mechanism, leaving the compliance burden on US firms themselves. Other countermeasures implemented by the US include export controls in the semiconductor sector, which the US tightened between 2022 and 2025, and blacklisting several Chinese entities from trade in semiconductors and advanced strategic technologies. Furthermore, the US used the Chip4 Alliance, a cooperative engagement with South Korea, Taiwan, Japan, and the Netherlands, to restrict the export of chip technology to China. The potential issues concern the fact that the US and its allies have shown they can update strategic semiconductor export controls once per year, while China's legal and illegal responses are much faster, as it is willing to make bold and expensive bets on short notice. Furthermore, equipment produced in overseas facilities can be legally sold to advanced logic fabrication factories in China, even if the customer is on the US entity list, creating a significant loophole.

Regarding Europe-level countermeasures, from March 2025, the EU has released two strategic frameworks: the European Defence Readiness 2030, which is an EUR 800b investment plan that targets Europe's capability gaps in drones, air defence, and AI-driven systems, and the EU Preparedness Union Strategy, which focuses on resilience and strategic autonomy. Furthermore, in November 2025, the European Democracy Shield was announced and, even if it is still in draft, it is expected to incorporate cybersecurity legislation in existing counter-disinformation bodies to target foreign interferenCE and malign influence operations. The potential issue for EU countermeasures lies in the EU's compartmentalised approach to cyber risks, which leaves European infrastructure exposed to synchronised campaigns.

The most historically proven countermeasure against an adversary who treats detection as an operational cost is not to eliminate known assets but to exploit them. The Double Cross System used by British intelligence in WWII turned German spies operating in Britain into a channel for controlled misinformation, feeding false data about invasion plans that directly shaped German strategic decisions. Applied to the MSS context, rather than immediately disrupting identified APT access points or arresting known HUMINT sources, Western agencies could allow penetrated agents to persist while carefully feeding false technical data, such as plausible but flawed ICBM system documents or misleading drone-swarm tactics.

Countermeasures

The payoffs would be limited MSS gains based on corrupted intelligence, and the West gained insight into the data China prioritises, thereby understanding its operational gaps. Specifically, the Typhoon campaigns pre-positioned their infrastructure access, allowing the West to exploit these operations and allowing China to believe it retains access while the access itself is being monitored and selectively manipulated.

Another countermeasure Western countries could consider is a multilateral Counter-Threat Network (CTN), like the Cold War precedent of multilateral CI cooperation developed by NATO from the 1950s to counter Soviet fragmented-agent networks of a similar structural type that the MSS now uses. The fragmentation of the adversary's network is only a vulnerability if the defender's network is more integrated. Currently, as seen in the Greek, French, and German cases, the EU's counterintelligence is operating in isolation, and the MSS is consistently exploiting this. A formal EU-level counterintelligence fusion cell, with mandatory cross–border case sharing on Chinese HUMINT operations (distinct from existing cybersecurity cooperation), would directly target the asymmetry that is currently characterising US and European detection effectiveness.

BLOOMSBURY INTELLIGENCE & SECURITY INSTITUTE

For more information, products and services

info@bisi.org.uk

www.bisi.org.uk

Bloomsbury Intelligence and Security Institute (BISI)

© 2026 Bloomsbury Intelligence and Security Institute

"Bloomsbury Intelligence and Security Institute" is the trading name of Bloomsbury Intelligence and Security CIC, registered in England and Wales (Company No. 16255943). It is currently not registered as an Institute under UK Law.