COMPETING WITHOUT FIGHTING

CHINA'S STRATEGY OF POLITICAL WARFARE

AUTHORS
Seth G. Jones
Emily Harding
Catrina Doxsee
Jake Harrington
Riley McCabe

A REPORT OF THE CSIS TRANSNATIONAL THREATS PROJECT CSIS CENTER FOR STRATEGIC & INTERNATIONAL STUDIES
China is conducting an unprecedented campaign below the threshold of armed conflict to expand the influence of the Chinese Communist Party (CCP) and weaken the United States and its partners. This campaign involves sophisticated Chinese espionage activities, offensive cyber operations, disinformation on social media platforms, economic coercion, and influence operations targeting companies, universities, and other organizations.

This report offers one of the most comprehensive analyses to date of Chinese political warfare activities and examines China’s main actions, primary goals, and options for the United States and its partners. It sheds new light on the scope and breadth of Chinese activities and comes to several conclusions.

First, China is conducting an increasingly active and aggressive campaign to penetrate a wide range of U.S. academic institutions, companies, government agencies, and nongovernmental organizations (NGOs). The scale of China’s actions in the United States is unparalleled. As one Federal Bureau of Investigation (FBI) senior official told the authors, “The system is blinking red right now. We have not seen this level of Chinese intelligence and influence activity in and around the U.S. homeland ever.”

Over the past year, for example, the FBI and Department of Justice (DOJ) have arrested or indicted numerous individuals for espionage, cyber operations, and illegal influence campaigns. The list includes an indictment against the codirector of a U.S.-based think tank for acting as an unregistered foreign agent for China and other actions, a series of aggressive cyberattacks against senior U.S. government officials and companies such as Microsoft, and the expansion of Chinese intelligence collection sites in such countries as Cuba.

In addition, China has been involved in an expansive campaign to monitor, harass, and coerce residents of the United States and other countries as part of an extralegal repatriation effort known as Operation Fox Hunt. In 2023, for example, the FBI arrested two individuals, “Harry” Lu Jianwang and Chen Jinping, in connection with operating an illegal police station in Manhattan, New York City, for China’s Ministry of Public Security (MPS). In 2023, DOJ also indicted dozens of MPS officials for conducting online intimidation against Chinese nationals residing in the United States who were critical of China.

Second, the report details that China’s top target for political warfare—by far—is the United States. Chinese actions against the United States are more expansive than is generally known and include:

- **Intelligence Operations**: China’s intelligence services, such as the Ministry of State Security (MSS) and MPS, are engaged in extensive human intelligence, signals intelligence, and other types of intelligence collection as part of political warfare—including intimidating Chinese diaspora in the United States. In examining over 100 Chinese espionage cases directed at the United States and U.S. entities, this report concludes that Chinese intelligence operations are not just pervasive, but they are used to plan and execute all of China’s other political warfare activities.

- **Cyber Operations**: Chinese organizations, including units within the People’s Liberation Army (PLA), are involved in a cyber campaign against U.S. and other international corporations, universities, government agencies, media, think tanks, NGOs, and other targets. These efforts are designed to help China leapfrog ahead of the West by skipping the extensive and time-consuming research and development phases for new technologies. China’s cyber operations are also intended to influence foreign and domestic audiences, assist with offensive military campaigns, and improve the country’s artificial intelligence and big data analytics capabilities.

---

1 Authors’ interview with FBI agent, June 2023.
Information and Disinformation Operations: China is engaged in extensive information and disinformation activities overseas—including in the U.S. homeland—designed to influence decisionmaking and popular support to gain a competitive advantage. Beijing seeks to tightly control the image of China abroad, including by influencing companies, organizations, and individuals that criticize China, from the National Basketball Association to Hollywood studios.

United Front Work: The CCP is involved in aggressive efforts to extend its reach overseas through united front work, which involves activity to protect and bolster the image of China and the CCP. United front work includes activities to influence individuals in such countries as the United States who are well positioned to amplify China’s preferred messaging on political, economic, and other issues.

Irregular Military Actions: The PLA Army, PLA Navy, PLA Air Force, PLA Rocket Forces, People’s Armed Forces Maritime Militia, research organizations, and private security companies linked to China are involved in widespread efforts to expand Chinese influence below the threshold of armed conflict. Chinese organizations are involved in near-seas activities (which focus on securing Chinese interests around such areas as the South and East China Seas) and far-seas activities (which are global in scope). This report constructs a dataset of Chinese private security companies that shows that there are nearly two dozen Chinese private security companies operating overseas, including in Africa, the Middle East, Asia, and Latin America.

Economic Coercion: China has penetrated—or attempted to penetrate—virtually every sector of the U.S. economy, as well as many of its partners such as the United Kingdom. In addition, China is engaged in the threat or imposition of economic costs or inducements to influence decisionmaking and popular support in other countries to gain a competitive advantage. There has been considerable focus on the Belt and Road Initiative as part of a broader effort to influence foreign governments. As this report highlights, however, another concerning Chinese initiative is the Digital Silk Road, which aims to spread Chinese influence through telecommunications, e-commerce, hardware, software, big data, artificial intelligence/machine learning, and other digital infrastructure across the globe.

These tools are part of a broad strategy of political warfare, which U.S. diplomat George Kennan described as “the employment of all the means at a nation’s command, short of war, to achieve its national objectives.” The U.S. public and other international audiences are often unaware of the full nature and scope of these Chinese activities, including those that target U.S. and other Western companies, government agencies, universities, news media, digital platforms, and other NGOs.

These tools are not mutually exclusive but are sometimes overlapping, reinforcing, and occasionally even duplicative and competitive. China presents a “whole-of-state” approach to political warfare. Multiple organizations are involved, such as the PLA, MSS, MPS, Ministry of Industry and Information Technology, United Front Work Department, and Ministry of Foreign Affairs. A wide range of non-state or quasi-state actors are also involved, from hacktivists to private security companies.

Third, China has several strategic goals in conducting political warfare. The most important is preservation of the CCP’s rule. Another is expanding Chinese influence and weakening the United States as part of balance-of-power competition. These goals are in line with China’s national strategy of achieving “the great rejuvenation of the Chinese nation on all fronts.” China also conducts political warfare—rather than armed conflict—to avoid conventional war and refrain from provoking other countries.

In light of these activities, the United States and its partners have been slow to identify and counter Chinese political warfare. This needs to change. Moving forward, there are several core components of an effective strategy to compete with China. One is grounding U.S. responses in democratic principles, which remain critical in a struggle with authoritarian regimes. A second is improving defensive measures, such as:


■ **Increase Federal Counterintelligence Resources**: Boost FBI, DOJ, and Department of Homeland Security (DHS) resources to conduct Chinese counterintelligence operations against the MSS, MPS, PLA, United Front Work Department, and other organizations. For example, the FBI should be given additional resources to hire more counterintelligence agents and intelligence analysts, including Mandarin-proficient personnel.

■ **Expand State and Local Counterintelligence Activities**: There is a growing need to supplement U.S. federal efforts by expanding state and local efforts. New Jersey, for example, has stepped up counterintelligence efforts under the New Jersey Office of Homeland Security and Preparedness. These efforts should be widespread across U.S. states.

■ **Strengthen Foreign Agent Registration Act (FARA) and Related Efforts**: There is a continuing need to further strengthen FARA and other efforts, including the Lobbying Disclosure Act and the Department of Education’s Section 117 disclosures, to counter Chinese and other foreign influence. Examples might include providing civil investigative demand authority to the Department of Justice, increasing penalties for noncompliance with registration requirements, and repealing or modifying FARA exemptions.

A third component is conducting a more effective offensive campaign. U.S. policymakers have been more comfortable with defensive measures to protect the United States from Chinese activities. But U.S. and partner offensive measures are also essential. Examples include:

■ **Weaken the Great Firewall**: The United States needs to increase resources and support to programs that provide technological and other assistance to individuals and organizations inside and outside China to break through the Great Firewall. These programs should include U.S. government agencies—such as the State Department, Defense Department, and intelligence community—as well as NGOs and the private sector.

■ **Establish a Multilateral Bloc to Counter Chinese Economic Coercion**: Combating and deterring Chinese economic coercion will require a collective effort by the United States, Australia, South Korea, Japan, India, and other countries—including in Europe. Participant countries should be prepared to sanction China in response to Chinese threats or actions that do not conform to World Trade Organization rules and are aimed at meeting Chinese political goals unrelated to trade. In addition, participant countries could create a collective compensation fund for losses and offer alternative export or import markets to divert trade in response to Chinese sanctions.

■ **Increase Private Sector Competitiveness in Emerging Technology**: Develop a public-private partnership designed to compete more effectively with China in emerging technology in such areas as the Global South. China has developed an aggressive strategy to spread Chinese technology through the Digital Silk Road. The United States and partner governments should develop a coordinated approach to support U.S. and partner companies that seek to compete in these same regions, such as Google, Amazon, Apple, and Microsoft.

Deepening relationships with partners is critical in all of these areas. For example, Australia blocked the purchase of Huawei 5G telecommunications gear for its national network and was an outspoken critic of China’s human rights abuses and anti-democratic practices. But the threat from China against U.S. partners is likely to be persistent.

At the beginning of the Cold War, Kennan authored a U.S. State Department Policy Planning Staff memorandum on political warfare that remains relevant to today’s competition with China. He noted that a significant part of great power competition involves activities below the threshold of conventional and nuclear warfare. Today, China is heavily involved in many of these activities. As this report documents, China also has significant weaknesses and vulnerabilities that can be exploited. Together with its partners, the United States now needs to develop a comprehensive approach to compete in this arena that is consistent with its democratic principles and values. The clock is ticking.

---

4 Kennan, “The Inauguration of Organized Political Warfare.”