Cyber Threats to the U.S. from China

Akela Villegas

August 26, 2025

CYSE 426: Cyber War

Abstract

As digital technology has become deeply integrated into today's society, cybersecurity threats have emerged as a significant challenge to national security. Among these threats, cyber operations originating from China pose some of the most persistent and strategically complex dangers to the United States. These threats are not limited to traditional espionage but also include intellectual property (IP) theft, influence operations, and cyber-enabled economic warfare. This paper explores the multifaceted nature of cyber threats posed by China to the U.S., analyzes the methods and motivations of Chinese cyber actors, and evaluates the effectiveness of existing U.S. countermeasures. Drawing on scholarly sources and government reports, the analysis reveals an effort by the Chinese state to leverage cyberspace for strategic advantage. The study concludes with recommendations for enhancing U.S. resilience through policy, diplomacy, and public-private collaboration.

Introduction

The rise of cyberspace as a strategic domain has transformed the nature of international conflict and competition. In recent years, the U.S. has increasingly been targeted by sophisticated cyber operations attributed to the People's Republic of China (PRC). These operations encompass a wide range of activities, including but not limited to intellectual property theft, cyber espionage, attacks on critical infrastructure, and influence campaigns. The strategic goals behind these operations align with China's broader geopolitical objectives, including its ambitions to become a global technological leader and to challenge the U.S.-led international order (Cooper, 2018).

At its core, this threat represents more than just technical challenges; it is a contest of influence, power, and economic dominance. The cyber domain offers China unique advantages like its ability to mask actors behind layers, scale attacks rapidly, and to blend state and non-state actors all complicate the U.S. response. For Americans, these attacks are not abstract; they impact everyday life, from the products we use to the security of our personal information.

The Chinese cyber threat landscape is uniquely challenging because it blends state-directed activities with operations conducted by proxies and semi-independent actors. Furthermore, the cyber domain allows for plausible deniability, complicating attribution and response strategies. As a result, the U.S. must adopt a comprehensive approach that addresses both the technical and strategic dimensions of the threat. This paper aims to dissect the nature of Chinese cyber threats, assess their implications for national security, and propose informed policy responses.

Understanding China's Cyber Strategy

China's cyber strategy is deeply rooted in its national development plans and military doctrine. The PRC views cyberspace as a critical domain for both economic and military competition. According to the White House (2023), China's cyber capabilities are considered among the most advanced and are often employed to support its broader national objectives, including economic modernization, military advancement, and political control.

The Chinese government has been transparent, in a rare way, about its ambitions. The 2017 "Made in China 2025" plan explicitly called for China to reduce dependence on foreign technology, aiming for self-sufficiency through innovation and acquisition. Cyber operations are

an integral component of achieving this, often by illicitly acquiring foreign intellectual property to shortcut research and development (U.S. IP Commission, 2019).

Chinese cyber strategy is heavily influenced by the concept of "civil-military fusion," wherein civilian technologies and companies are integrated into the national defense infrastructure. This approach enables the Chinese government to leverage the capabilities of its thriving tech sector for cyber operations(Nicholas, 2024). State-sponsored groups, such as APT41, exemplify this fusion by conducting operations that serve both state and criminal objectives (Kianpour, 2021). These groups often engage in IP theft, surveillance of dissidents, and strategic reconnaissance of critical infrastructure. The U.S. believes that China is responsible for over 90 percent of cyber-enabled intellectual property theft in the United States. In Table 2 on page 4, there is a summary of the significant IP thefts by the Chinese against U.S. businesses and organizations in 2019. “The incident reported in August is related to the theft of protected data from multiple U.S. cancer institutes by Chinese state-sponsored hackers as a part of APT41 operations. Healthcare research centers have been frequently targeted by Chinese cyber attacks in last decades. Cancer-related research institutes, in particular, are becoming more popular targets for Chinese APT groups, reflecting the growing concerns of China over dramatically increasing cancer incidence and mortality rates, and the Five-Year economic development plans” (Kianpour, 2021).

Additionally, China employs a "whole-of-society" approach to cyber operations. Universities, research institutes, and even private companies are expected to contribute to national security goals. This systemic mobilization enables China to conduct cyber campaigns with scale, precision, and persistence that few nations can match. It also allows the Chinese

government to maintain a degree of separation from the actors involved, thus complicating attribution.

This multi-faceted approach reflects the Chinese view that cybersecurity is not just a matter of technical defense but a comprehensive strategic tool. The government emphasizes integrating cyber capabilities into the broader national power structure, making cyber operations a key pillar of China's strategic competition with the U.S.

Profile of Threat Actors

A key aspect of China's cyber threat landscape is the diversity of actors involved. These include state agencies like the Ministry of State Security (MSS) and the People's Liberation Army (PLA), as well as civilian proxies and criminal groups. Each of these actors plays a distinct role in China's cyber ecosystem.

The MSS is primarily responsible for foreign intelligence, economic espionage, and monitoring political dissent, typically operating through regional bureaus and collateral civilian networks. The PLA, particularly its Strategic Support Force, focuses on cyber, electronic, and psychological warfare capabilities under centralized military control, particularly on military intelligence, reconnaissance, and offensive cyber capabilities (Costello & McReynolds, 2019).

Meanwhile, groups like APT41 operate at the intersection of state and criminal objectives, blending espionage with financially motivated hacking. APT41 is notable for its wide-ranging cyber intrusions targeting technology, healthcare, and telecommunications sectors, often to steal intellectual property and sensitive data. These operations blur the lines between state priorities and personal financial gain, complicating efforts to categorize and respond to threats (Kianpour, 2021).

The decentralized nature of these operations provides China with flexibility and deniability. It also presents a challenge for U.S. policymakers, who must contend with a threat that is both state-directed and criminally opportunistic. Moreover, the proliferation of cyber capabilities within China's broader society means that the threat is not limited to a few elite units but is systemic in nature.

Notable Cyber Incidents

Several high-profile cyber incidents illustrate the scale and sophistication of Chinese cyber operations. One of the most significant was the 2015 Office of Personnel Management (OPM) breach, which resulted in the theft of sensitive personal data of over 21 million U.S. federal employees. Investigators linked the attack to actors connected with China's Ministry of State Security (MSS), highlighting just how intricate and deep Chinese cyber operations can penetrate critical U.S. systems (Finklea & Christensen, 2015).

The stolen data did not just include names and addresses, but also background checks and security clearance information. This breach had wide-ranging implications which could be used for blackmail or to identify intelligence operatives. The OPM hack signaled the seriousness of Chinese cyber espionage targeting the U.S. government infrastructure.

Another major incident was the Equifax breach in 2017. "The nine-count indictment alleges that Wu Zhiyong, Wang Qian, Xu Ke and Liu Lei were members of the PLA's 54th Research Institute, a component of the Chinese military. They allegedly conspired with each other to hack into Equifax's computer networks, maintain unauthorized access to those computers, and steal sensitive, personally identifiable information of approximately 145 million American victims" (Office of Public Affairs, 2025).

The 2021 Microsoft Exchange Server hack exploited zero-day vulnerabilities (CVE-2021-26855 and others) to gain access [T1190] to on-premises Microsoft Exchange servers of U.S. entities that allowed attackers to gain access to email accounts and install web shells for persistent control. The U.S. and allies attributed the campaign to a Chinese state-sponsored group known as Hafnium, believed to operate on behalf of China's Ministry of State Security (MSS). The attack compromised tens of thousands of organizations worldwide, highlighting China's ability to rapidly weaponize newly discovered vulnerabilities for large-scale cyber operations (CISA, 2021).

Beyond theft, these intrusions demonstrate China's ability to disrupt, surveil, and potentially sabotage critical U.S. networks. The combination of intellectual property theft and strategic reconnaissance presents a broad threat spectrum that the U.S. must contend with across both civilian and military domains.

Influence Operations and Psychological Warfare

Beyond espionage and data theft, China has developed capabilities for influence operations and psychological warfare in cyberspace. These campaigns are designed to shape public opinion, manipulate narratives, and undermine trust in democratic institutions. Chinese influence operations often exploit social media platforms, where they disseminate disinformation and amplify divisive content.

China seeks to influence American discourse through covert propaganda. These efforts are not limited to election interference but extend to promoting favorable narratives about China and discrediting its adversaries. Tactics include using fake social media accounts, automated bots, and content farms to spread state-approved messaging. These influence operations are

carefully calibrated to avoid direct attribution while maximizing impact on public opinion. For example, during the COVID-19 pandemic, Chinese-linked campaigns spread disinformation to deflect blame and promote the Chinese government's pandemic response. China engaged in a coordinated disinformation campaign, promoting theories such as the possibility that the U.S. military introduced the virus to Wuhan, while simultaneously highlighting its own pandemic response as responsible and effective. These messages were disseminated via state-controlled media and amplified across social media platforms, with dissenting narratives actively suppressed (Case, 2020).

The Economic Implications of Cyber Espionage

China's cyber activities have profound economic consequences for the U.S. economy. Intellectual property theft, in particular, has been a central feature of Chinese cyber strategy. According to the Commission on the Theft of American Intellectual Property, the U.S. economy loses between $225 billion and $600 billion annually due to IP theft, much of which is attributed to Chinese cyber operations (Wiseman, 2023).

The ramifications extend beyond the private sector. For example, Chinese cyber espionage targeting pharmaceutical companies threatens U.S. leadership in healthcare innovation. Similarly, attacks on manufacturing technology impede the competitiveness of American industry, potentially shifting economic power in favor of China. These economic impacts emphasize the urgency of addressing cyber threats through a combination of technical defenses, legal measures, and international cooperation.

U.S. Policy Responses

In response to the growing cyber threat from China, the U.S. has implemented a variety of defensive and offensive measures. These include indictments of Chinese hackers, diplomatic protests, and the imposition of sanctions. While such actions signal U.S. resolve, they have had limited success in deterring Chinese cyber aggression.

One promising development is the implementation of the Zero Trust cybersecurity framework across federal agencies. This model assumes that threats can originate from both inside and outside the network and emphasizes continuous verification of user identities and device health (CISA, 2021).

The U.S. has also increased funding for cybersecurity research and workforce development. The Cybersecurity and Infrastructure Security Agency (CISA) plays a vital role in coordinating efforts to defend critical infrastructure and disseminate threat information. However, challenges remain, particularly in coordinating efforts across the public and private sectors, such as resource gaps and information sharing barriers. The complexity and scale of the Chinese cyber threat require a whole-of-nation approach that leverages the capabilities of all stakeholders. This approach includes encouraging private companies to improve their cyber defenses, enhancing public awareness, and fostering greater cooperation between government and industry.

The Human Element in Cybersecurity

It is essential to recognize that cyber threats are not only about technology but also about people, those who create, defend, and exploit digital systems. Chinese cyber operations often exploit human vulnerabilities such as weak passwords, phishing scams, and insider threats. Social engineering remains a powerful tool for attackers, allowing them to bypass sophisticated

technical defenses by manipulating human behavior. This underscores the importance of cybersecurity awareness and training as a critical component of any defense strategy.

Moreover, the challenge for U.S. policymakers is not just technical but also organizational and cultural. Cybersecurity requires seamless coordination across agencies, private companies, and international partners. Yet, barriers like withholding information, bureaucratic inactivity, and differing priorities often hinder effective cooperation. A Department of Homeland Security Office of Inspector General (OIG) report revealed that participation in the Cybersecurity and Infrastructure Security Agency's (CISA) Automated Indicator Sharing (AIS) program declined from 304 participants in 2020 to only 135 in 2022, a 93% decrease in shared cyber threat indicators. The report notes that the decline in sharing occurred largely "because a key Federal agency" stopped sharing threat intelligence "due to unspecified security concerns with transferring information from its current system to AIS" (Greig, 2024). Bridging these gaps is as important as technological upgrades and can often determine the success or failure of a cyber defense initiative.

The Strategic Importance of Cyber Deterrence

Deterrence in cyberspace remains an evolving and challenging concept. Unlike traditional military domains, where physical destruction is clear and immediate, cyberattacks are often stealthy and ambiguous. This ambiguity complicates retaliation and risk assessment. China's strategy of plausible deniability and use of proxy actors means that the U.S. must develop innovative deterrence models that combine diplomatic, economic, and cyber means. The U.S. employed a multifaceted deterrence strategy against Chinese cyber espionage, combining public attribution and diplomatic signaling, criminal indictments with economic consequences, and cyber countermeasures, as illustrated by the 2018 arrest of Su Bin for stealing aircraft

designs. These measures collectively elevated the cost of cyber intrusions for China and contributed to a subsequent reduction in such operations (Graff, 2018).

Cyber deterrence also requires clear communication of red lines and consequences. Without credible threats of retaliation, adversaries may perceive cyber operations as low-risk, incentivizing further aggression. The U.S. has begun exploring “defend forward” policies which means taking proactive measures to disrupt adversary operations before they cause harm, but these raise complex legal and ethical questions that require careful consideration.

International Collaboration and Future Recommendations

Given the global nature of cyberspace, international collaboration is essential for countering Chinese cyber threats. The U.S. has strengthened ties with allies through initiatives like the Quad (with India, Japan, and Australia) and NATO’s new cyber defense strategies. These alliances enhance information sharing and facilitate coordinated responses to cyber incidents.

Additionally, the U.S. should lead efforts to establish international norms for responsible behavior in cyberspace. This includes advocating for agreements that prohibit cyberattacks on critical infrastructure and promote accountability for state-sponsored hackers. Diplomatic engagement with China should also be pursued, though it must be grounded in clear red lines and credible consequences for violations.

Domestically, the U.S. must continue to invest in cybersecurity education and public awareness. Building a resilient cyber ecosystem requires not only technical solutions but also a cyber-literate populace. Public-private partnerships should be deepened to ensure that threat intelligence flows seamlessly across sectors.

Finally, the U.S. must maintain its technological edge through investments in quantum computing, artificial intelligence, and secure communication networks. These technologies will shape the future of cyber conflict and determine the strategic balance in the years to come.

Conclusion

The cyber threat from China represents one of the most pressing national security challenges of the 21st century. With a sophisticated and multifaceted strategy, China has exploited vulnerabilities in cyberspace to conduct espionage, steal intellectual property, and wage influence campaigns. The U.S. must respond with equal complexity, combining technological innovation, strategic policy, and international collaboration.

While progress has been made, much work remains to be done. A comprehensive response to Chinese cyber threats will require sustained investment, political will, and societal resilience. By adopting a proactive and integrated approach, the U.S. can safeguard its digital future and uphold the values of openness, innovation, and democracy.

References

Cooper, Z. (2018, September 5). Understanding the Chinese Communist Party's approach to cyber-enabled economic warfare. *American Enterprise Institute*. https://www.fdd.org/analysis/2018/09/05/understanding-the-chinese-communist-partys-approach-to-cyber-enabled-economic-warfare/

Case, J. (2020, December). *Telling China's COVID-19 Story Well: Beijing's Efforts to Control Information and Shape Public Narratives Regarding the 2020 Global Pandemic* . CNA. https://www.cna.org/archive/CNA_Files/pdf/drm-2020-u-028558-final.pdf

CISA. (2021, March 10). Compromise of Microsoft Exchange server. https://www.ic3.gov/CSA/2021/210310.pdf

Costello , J., & McReynolds, J. (2019, February 5). *China's Strategic Support Force: A force for a new era*. National Defense University Press. https://ndupress.ndu.edu/Media/News/News-Article-View/Article/1748555/chinas strategic-support-force-a-force-for-a-new-era/

Cybersecurity and Infrastructure Security Agency (CISA). (2021). *Zero Trust Maturity Model*. https://www.cisa.gov/zero-trust-maturity-model

Finklea, K. F., & Christensen, M. D. (2015). *Cyber Intrusion into U.S. Office of Personnel Management: In Brief.* Congressional Research Service.

Graff, G. M. (2018, October 11). *How the US forced China to quit stealing-using a Chinese spy*. Wired. https://www.wired.com/story/us-china-cybertheft-su-bin/

Greig, J. (2024, September 30). *CISA pledges to resolve issues with threat sharing system after watchdog report*. Cyber Security News | The Record. https://therecord.media/cisa pledges-to-resolve-threat-sharing-program-issues-oig-report

Kianpour, M. (2021, March 8). Socio-technical root cause analysis of cyber-enabled theft of the U.S. Intellectual Property — the case of APT41. *arXiv*. https://arxiv.org/abs/2103.04901

Liyanage, L., Arachchilage, N., & Russello, G. (2025, April 7). *A novel framework to assess cybersecurity capability maturity*. arXiv.org. https://arxiv.org/abs/2504.01305

Nicholas , A. (2024, September 30). *China's military-civil defusion*. The Wire China. https://www.thewirechina.com/2024/09/22/chinas-military-civil-defusion/

Office of Public Affairs. (2025, February 6). *Chinese military personnel charged with computer fraud, economic espionage and wire fraud for hacking into credit reporting agency Equifax*. Office of Public Affairs | Chinese Military Personnel Charged with Computer Fraud, Economic Espionage and Wire Fraud for Hacking into Credit Reporting Agency Equifax | United States Department of Justice. https://www.justice.gov/archives/opa/pr/chinese-military-personnel-charged-computer fraud-economic-espionage-and-wire-fraud-hacking

White House. (2023). *National Cybersecurity Strategy*. https://bidenwhitehouse.archives.gov/wp-content/uploads/2023/03/National Cybersecurity-Strategy-2023.pdf

Wiseman, P. (2023, December 1). *Counterfeiters, hackers cost us up to $600 billion a year*. AP News. https://apnews.com/counterfeiters-hackers-cost-us-up-to-600-billion-a-year2234bddc68c14ba18d4d403442187c59