Chinese Cyber Espionage: Intellectual Property Theft, the Silent War against the West

Christopher Sicle

Old Dominion University School of Cybersecurity

CYSE 426: Cyber War

Dr. Russell A. Korb

July 25, 2025

Abstract

This paper examines China's strategic use of cyberwarfare as a modern tool for its quest to become a cyber superpower, focusing on its coordinated campaigns of intellectual property (IP) theft, cyber espionage, and human intelligence (HUMINT). Seeking a different method of warfare beyond kinetic options, China's cyber strategy is designed to achieve long-term gains, specifically by accelerating its military modernization and economic competitiveness without incurring the high costs associated with research and development. The paper will analyze pillar entities such as the People's Liberation Army Strategic Support Force (PLA SSF) and the Ministry of State Security (MSS), which coordinate offensive cyber operations and insider recruitment. We will cover recent cases of espionage, like the 2023 arrests of U.S. Navy sailors passing information to Chinese agents, showing the dedication to the use of HUMINT. Additionally, this paper examines the paradox of China's continued reliance on Western technology, particularly Microsoft systems, and how such dependence could become a strategic point of leverage in future conflicts. The findings suggest that cyberwar is not an emerging threat; it is already here, reshaping national security, sovereignty, and the global digital ecosystem. The United States must adapt its policies and partnerships to address this evolving, non-traditional battlefield.

Introduction

Today's world has quickly developed into a digitally dependent society, and cyberwarfare is no longer a threat scene in sci-fi films, but rather an active, evolving battleground where state and non-state actors collide in conflict without a single shot being fired or heard. One of the most prominent and persistent actors in this new modern conflict is the People's Republic of China's (PRC) long-term cyber campaign against the United States. Long gone are the days of the Korean War, when the US and PRC clashed in kinetic military force; now China has adopted cyberwarfare, emphasizing the advantages of stealth, persistence, and economic gain. China has leveraged these advantages primarily through cyber espionage and the theft of intellectual property (IP). With the effort of stealing Western IP, China has accelerated its military modernization and technological advancements by exfiltrating sensitive data within defense contractors, private firms, and critical infrastructure networks to compete with the US and Russia.

China distinguishes its cyber strategy with a hybrid approach that combines digital operations with human intelligence and tiptoeing around laws. Recent examples of Chinese nationals charged with espionage in the U.S. Navy illustrate how Beijing is combining modern cyber tactics with more traditional espionage techniques to gain a military advantage. These actions and strategies are putting strain on the West's current policies, military doctrines, and legal frameworks, which have been shaped for traditional warfare. Additionally, concerning is China's reliance on Western technologies, including Microsoft Operating Systems (OS) and various cloud infrastructure. This raises a curious question: if US-China geopolitical issues arise, how would these Western giant tech companies respond in the event of open conflict? Could

their platform be weaponized? Should they limit access to adversarial states? And how does this shape the future of digital sovereignty?

In this paper, we argue that China's cyber IP theft and espionage campaign constitutes a new form of cyberwar. One that is strategic, persistent, and deeply connected to the digital commercial ecosystem, the US must adapt and reevaluate the boundaries between military and commercial technology, recognizing that national security relies on securing cyberspace.

China's Cyber Strategy

Areas of conventional warfare, where military strength is projected through physical force and force projections. The PRC has been very public about its gains in conventional warfare and is building a robust military complex; however, it has also adopted a more covert model of conflict: cyber warfare. Over the last 20 years, Chinese leadership has heavily invested in operations in cyberspace, focusing not on destruction, but on disruption, espionage, and long-term strategic gain. With recent persistent cyber operation campaigns, China has aimed to narrow the gap with the West and gain informational dominance in future conflicts.

At the center of the People's Liberation Army (PLA) cyberwarfare effort is the People's Liberation Army Strategic Support Force (PLA SSF), established in 2015 to consolidate China's electronic warfare, cyber operations, and space capabilities under a single command. The U.S. Department of Defense (2022) identifies the SSF as the core organization responsible for both offensive and defensive cyber missions, including data exfiltration, network disruption, and support for conventional military operations (U.S. Department of Defense, 2022, pp. 68). Similar to the US structure of the National Security Agency and USCYBERCOM, PLA SSF's centralized structure enables efficient integration of cyber activities aligned with broader military and information warfare objectives.

"Cyber sovereignty" refers to the concept that states have complete control over their information space and digital infrastructure. Cyber sovereignty is a defining characteristic of China's cyber strategy. According to cybersecurity expert Adam Segal (2020), China pursues cyber sovereignty both domestically, through mass censorship and surveillance, and internationally, by advocating for global internet governance norms that legitimize authoritarian control of cyberspace. This mentality of the framework extends past just internal policy; it also supports China's ambition of becoming a global superpower in cyber capability by controlling the flow of data within and outside its borders.

China's cyber strategy is often described as "hybrid warfare," blending traditional statecraft with new digital tools. China's goal is not overt cyberattacks with destructive results, but rather long-term infiltration and data attractions utilizing affiliated groups from the Ministry of State Security (MSS) or the PLA. For example, the APT10 group executed a global hacking campaign known as "Cloud Hopper," which penetrated managed service providers and accessed sensitive intellectual property from dozens of U.S. and allied companies. In 2018, the U.S. Department of Justice indicted two Chinese hackers for their involvement, explicitly linking them to the MSS (U.S. Department of Justice, 2018).

This type of cyberwarfare does not rise to the level of armed conflict, making retaliation legally and politically difficult and indecisive. Operating in this gray area allows China to navigate around legal gaps, potentially conducting espionage without triggering a war response. These operations blur the line between criminal hacking and acts of war, especially when carried out under state sponsorship with military objectives.

Additionally, the PLA's cyber strategy relies on a combination of military and civilian sector capabilities, enabling China to leverage the technology sector's capabilities. As Segal

(2020) notes, Chinese law requires companies to cooperate with state intelligence services, effectively turning private industry into an extension of national security. This collaboration provides the SSF and MSS with access to next-generation commercial technology and infrastructure. By leveraging civilian cyber operations, China can expand its global espionage footprint.

China's cyber strategy represents a new defining aspect of warfare in modern times, by trading physical face-to-face confrontation for long-term covert influence, intellectual property theft, and infiltration. The PLA's SSF is the tip of the spear, enabling China to pursue cyber dominance.

Intellectual Property Theft Warfare

China's cyber operations are not strictly about disabling enemy systems or infiltrating secure intelligence; rather, a critical objective is the theft of intellectual property (IP). Unlike traditional espionage actions targeting state secrets, cyber IP theft by China specifically targets private industries, research institutions, and technology firms. The actions are not taken because they can. Instead, they are directed by state policy to accelerate economic and military technological development, specifically to avoid the immense time and cost associated with research and development. In this way, IP theft is a paramount pillar of China's cyberwarfare doctrine. According to the U.S. Department of Justice (2018), Chinese hacking groups such as APT10, operating under the MSS, have been responsible for some of the largest corporate data breaches in history. Going back to the Cloud Hopper campaign, which targeted managed service providers (MSPs) that served third-party IT vendors for large corporations and government agencies. With the MSPs compromised, APT10 gained access to a variety of files and directories containing proprietary information, technical documents, designs, and business plans from over a

dozen companies across multiple industries, including aerospace, biotechnology, and communications. With the stolen data, the Chinese government was able to repurpose the information, giving its institutions a head start in contributing to the state's long-term strategy.

This approach to cyberwarfare has brought consequences to the United States, with annual estimates reaching billions of dollars. More concerning, however, is the severe threat to national security. For example, when defense contractors are explicitly targeted, the stolen designs can be used for their military development. The J-20 stealth fighter jet is often compared to the United States' ace of the sky, the F-22 Raptor. These two jets bear suspicious similarities, and it is widely believed that cyber espionage played a role in the acquisition of the technology. In addition, the new addition to the Chinese Navy, the Fujian aircraft carrier, shares shocking similarities and capabilities with the United States Navy's flagship Ford-class carriers.

The U.S. Department of Defense (2022) emphasizes that China's cyber theft campaigns are closely coordinated with its military modernization efforts. The SSF and MSS collaborate to identify high-value industrial targets whose intellectual property can serve both commercial and dual-use military purposes (U.S. Department of Defense, 2022, pp. 67-69). Utilizing state-level resources, China conducted methodical and robust intelligence-gathering operations.

An area of great challenge when trying to counter cyber IP theft is the legal gray areas that surround it. IP theft does not reach the level of triggering a formal retaliation, where a kinetic strike would be a feasible option for deterrence. The actions taken, such as sanctions, indictments, and protests, have had little effect in deterring operations, as they continue to occur. Additionally, when IP is stolen, it cannot realistically be recovered. Once the technical plans or the inner workings of a software system are taken, they can be copied, modified, and redeployed,

causing the victim permanent consequences and losses that cannot be undone, while the attackers gain a wealth of knowledge.

IP theft is central to China's "Made in China 2025" initiative, a strategic plan that aims to bolster the country's advanced technology to move up the global value chain. Specifically, it focuses on artificial intelligence, semiconductors, robotics, and aerospace engineering. China's economic policy and cyberwarfare strategy demonstrate that the integration of intellectual property theft is closely tied to national ambitions. Cyber operations are enabling this development, altogether avoiding market competition (Qin, 2018).

In short, China's strategy of intellectual property theft is a quiet and persistent form of warfare. Intellectual property theft undermines the West's advantage, damages its technology industry, and all this without crossing into physical conflict. Intellectual Property theft is a form of cyber warfare, but rather than the battlefield being servers or code, it is innovation itself.

Human Intelligence Cyberwar

We have discussed China's ability to commit digital intrusions and the presence of sophisticated state-sponsored hacker groups. It has become increasingly clear that these operations are enhanced when human intelligence (HUMINT) methods are added. The implementation of cyber and HUMINT creates a hybrid strategy where IP theft, insider recruitment, and espionage serve as the primary goals. China has leveraged human assets embedded in critical areas, such as essential industries and the military of adversarial nations, to support its cyber operations.

According to the Center for Strategic and International Studies (2023), there have been 224 reported instances of Chinese espionage against the United States since 2020. Focusing on an incident that took place in 2023, two active-duty U.S. Navy sailors, Jinchao Wei and Wenheng

Zhao, were arrested and charged with transmitting sensitive national defense information to Chinese intelligence officers. Wei, who held a U.S. security clearance, was stationed on the USS Essex and passed along details about ship movements, weapons systems, and defense exercises. These incidents reveal that China is not merely hacking into systems; it is placing people in positions of trust to gather data that even sophisticated cyber tools may not access.

The actions of the HUMINT bridge the gap in cyber capabilities, especially when systems are air-gapped or when information is passed through word of mouth. According to the U.S. Department of Defense (2022), China's MSS oversees the network that includes professional intelligence officers, recruited insiders, and coerced overseas Chinese nationals. These actors support PLA SSF operations by identifying cyber vulnerabilities, facilitating insider access, and exfiltrating physical media or secure credentials (DoD, 2022, pp. 138-140).

The major concern is that HUMINT operations can compromise even the digitally robust military and commercial systems, including defense contractors, research universities, and IT administrators in critical technology infrastructure. Through a tactic known as "talent recruitment," formalized in programs like China's Thousand Talents Plan, which aims to recruit top-skilled professionals (DoD, 2022, pp. 139). All the while, some participants may believe they are engaging in lawful exchanges, and others know that they are passing on restricted information.

When human and cyber intelligence are combined, it creates a formidable threat, primarily targeting a nation like the United States, where its openness and individual freedom can be exploited. The US may have the most advanced network defenses, but when the human element is compromised, no system can be impenetrable.

Dependence on Western Tech

China's cyber operations heavily use the technology it wants to exploit. While China constantly promotes technological independence, as mentioned in its "Made in China 2025" strategy. China's government functions heavily rely on Western technology platforms, such as Microsoft. The dependence raises serious questions about what would happen in the event of an open war or an escalated cyber war with an adversarial nation. Can or will tech giants like Microsoft continue to provide services? Can it become a strategic vulnerability or a tool of leverage?

Despite China's goal for cyber sovereignty, Microsoft remains a paramount company in its digital infrastructure. Relying on Windows operating systems, Microsoft Office, and Azure cloud services in both the private and public sectors. Microsoft regularly reports that China is among the most active state actors in terms of cyberattacks against Western targets. The Chinese economy and government continue to rely on these Western-origin platforms (Microsoft, 2021). This introduces an interesting paradox that China's cyber infrastructure is partially built on the very infrastructure it targets.

The dependence on Western technology creates a double-edged sword scenario. It offers China familiarity and expertise with Western systems and vulnerabilities that can be exploited, as they have access to this knowledge. On the other hand, it does introduce risk when utilizing Western systems. In the event of open hostilities or cyberwar, this reliance on Western systems can be leveraged strategically if Microsoft and other US firms could be compelled to cut access and or disable software updates. This could lead to severe disruptions in the military, economic, and industrial sectors (Segal, 2020). As the U.S. Department of Defense (2022) notes, China's

digital modernization efforts still have heavy "reliance on foreign supply chains that have proven to be economic chokepoints" (DoD, 2022, pp. 18).

China is recognizing this vulnerability and has accelerated efforts in fostering a domestic solution. Initiatives such as the Huawei HarmonyOS, the "China Software Initiative," and the forced transition away from foreign software in Chinese state agencies reflect a strategic intent to reduce Western dependency (Segal, 2020). These efforts are still in their infancy, and most Chinese systems will continue to rely on Western technologies.

Ultimately, the issue of cyber sovereignty is evolving. Control over technology infrastructure is as critical as control over territory, and China has recognized this. Currently, the cyber war landscape, when escalations arise, will shift from stealing data to the power of access. This raises additional questions, such as: What will U.S. companies like Microsoft do? Going into the future, technology firms may play a pivotal role in cyber conflict.

Conclusion

China's cyber warfare strategy is adapting to the changing nature of modern conflict. Rather than focusing solely on physical military might, China is levergeing intellectual property theft, espionage, and HUMINT to achieve long-term economic and technology advancement gains. These operations greatly benefit both the private and public sectors, as they avoid the immense costs associated with the extensive research and testing that China is currently undertaking to modernize its military rapidly.

Through a hybrid model combining digital intrusions with insider recruitment, China has exploited gaps between the public and private sectors. Its campaigns often fall below the threshold of war, making retaliation difficult while still causing significant harm to U.S. innovation and security.

At the same time, China still relies on certain Western technologies, such as those from Microsoft and cloud platforms. This reliance presents both risk and opportunity for China and the West. In future conflicts, China can leverage its knowledge to conduct attacks on US technology, as both countries use the same software. However, it can spin back, and the US firms may decide to block access and new updates.

Ultimately, China's cyber operations are not isolated incidents but part of a broader and deliberate strategy. As cyber and traditional domains converge, the U.S. must adapt by redefining the roles of technology firms, closing legal gaps, and preparing for a form of warfare where the battlefield is digital and constant.

Refrences

Center for Strategic and International Studies. (2023). *Survey of Chinese espionage in the United States since 2000*. Strategic Technologies Program. https://www.csis.org/programs/strategic-technologies-program/survey-chinese-espionage-united-states-2000

Qin, L. W.-T. (2018). *Made in China 2025: China's strategy for becoming a global high-tech superpower and its global implications*. *Journal of Strategic Security, 13*(3), Article 1. https://doi.org/10.5038/1944-0472.13.3.1833

Segal, A. (2020). *China's vision for cyber sovereignty and the global governance of cyberspace*. National Bureau of Asian Research Special Report #87. https://www.nbr.org/publication/chinas-vision-for-cyber-sovereignty-and-the-global-governance-of-cyberspace/

U.S. Department of Defense. (2022). *Military and Security Developments Involving the People's Republic of China 2022: Annual Report to Congress* (pp. 126–139). https://media.defense.gov/2022/Nov/29/2003122279/-1/-1/1/2022-MILITARY-AND-SECURITY-DEVELOPMENTS-INVOLVING-THE-PRC.PDF

U.S. Department of Justice. (2018, December 20). *Two Chinese hackers associated with the Ministry of State Security charged with global computer intrusion*

campaign targeting intellectual property and confidential business information.

https://www.justice.gov/opa/pr/two-chinese-hackers-associated-ministry-state-security-charged-global-computer-intrusion