Securing China's Digital and Technological Strength

Anna Bateh

Political Science Department

POLI 3610: Asian Politics

Dr. Clary

April 21, 2025

Executive Summary

There is no relationship as significant to the future world of politics as that between the U.S. and China [1]. No other two nations play such dominant roles in critical global issues. How these two powers manage their relationship will likely be a key determinant of not only their own political and economic futures, but also wider global stability and prosperity [1]. In recent years, cybersecurity has become a crucial point of tension between China and the United States. Both nations continue to accuse each other of escalating digital espionage campaigns [7]. China has been at the center of this competition [7]. Recently, the U.S has implemented policies to limit China's technological reach by imposing trade restrictions, banning Chinese-owned apps, and using cybersecurity concerns to justify excluding Chinese companies. China has faced ongoing cyber threats from the U.S, posing risks to its national security.

Furthermore, the United States has been accused of targeting Chinese companies through espionage to steal sensitive data. These external threats underscore China's ability to develop complex technology. It could threaten national security if China does not address foreign cyberattacks and technological dependencies. China must prioritize technological independence to overcome obstacles from the United States. To address these challenges, China must reduce its reliance on foreign technology. This memo suggests that for China to maintain its external threats, it must strengthen its cybersecurity infrastructure, invest in domestic technology innovation, and create an agenda with the United States to create possible solutions. These steps are essential to protect China's digital future and secure its long-term technological independence.

Background/ Context:

In May 2023, China's National Computer Network Emergency Technical Team (CNCERT/CC) accused a U.S[5]. intelligence agency of launching cyberattacks on two Chinese tech firms. The first attack targeted a Chinese company that was focused on advanced material organization [5]. U.S hackers exploited a weakness in a document security system and used it to install malware through a software update, allowing them to take control of over 270 computers to steal important trade secrets and research [5]. The second attack was on a company in the smart energy and digital information industry where U.S.-linked hackers, known as Volt Typhoon and Salt Typhoon, broke into the company's email system, planted backdoor programs, and stole large amounts of sensitive data [5].

These attacks, aimed at stealing commercial secrets and intellectual property, have had the effect of raising serious concerns over Chinese national cybersecurity. The intrusion, which lasted for four months from April to August 2024, allowed the US attackers to maintain a persistent presence on the organization's network for intelligence-gathering purposes [5].
This is only a glimpse of the ongoing cybersecurity issue between the United States and China; ultimately, these examples reflect a much larger concern. As the United States continues to put pressure on China's access to technologies such as semiconductors and AI, cybersecurity threats against Chinese companies have increased [5]. Many of these incidents prove how serious the risks are to China's national security and technological independence [5].

Problem:

China's reliance on foreign technology and firms' vulnerability to cyber espionage have undermined its technological capabilities. Over the past decade, the U.S. has built an extensive number of regulatory tools to regulate U.S. data flows to China [2]. The United States has capitalized on China's technological weaknesses, such as intellectual property threats and forced technology transfers, to enforce measures that undermine China's technological goals. This has posed a serious threat to China's future, both economically and technologically [2].

External Cyber Threats to China's Technological Strength:

The United States has used cybersecurity concerns as a means for imposing restrictions on Chinese technologies. Therefore, they have taken several steps in recent years to limit Chinese access to critical data. The United States views this as a loophole for potential espionage and cyberattacks. This section highlights the external cyber threats the United States poses and how they directly affect China's national security and technological independence [2].

1. **Banning Chinese-owned apps and devices:** On January 20, 2025, President Donald Trump sought to delay a 2024 law banning the Chinese-owned app, TikTok [2]. President Trump aimed to negotiate a deal with TikTok's owner, ByteDance, asking them to give up control of the app to reduce national security concerns regarding data privacy and Chinese governmental influence [2]. This delay reflects U.S efforts to restrict or ban Chinese communication technologies, software, and internet-connected devices. Over the past twelve months, the U.S restricted Chinese cargo cranes, limited data transfers, and

drafted rules to ban Chinese drones and other vehicles [2]. These actions signify an ongoing strategy to reduce China's technological influence [2].

2. **Cybersecurity as a Strategic Tool:** The U.S has used its cyber capabilities to gather Chinese intelligence [2]. Although the incident in May of 2023 helps to prove this point, there have been other cases where China has accused the United States of stealing a Chinese company's sensitive data [2]. Cyberattacks weaken China's technological strength by disrupting its ability to innovate [2]. Stealing valuable research leads China to face an increasing risk of technological independence [2].
3. **Trade Enforcement and Legal Pushbacks:** The United States has taken strong action to address what it believes are 'unfair Chinese trade practices' such as intellectual property theft and forced technology transfers [7]. Under Section 301 of the Trade Act of 1974, the United States imposed an additional 25% tariffs on approximately $50 billion of products from China that are strategically important to, and benefit, the "Made in China 2025" program and other industrial policies [8]. The U.S response through tariffs on Chinese technology is a direct example of how they are trying to curb China's technological and economic growth; ultimately, the United States is actively using these tools to protect its technological goals.

Opportunities:

Despite many threats from the U.S, there is an opportunity for China to overcome these challenges. China can invest in the domestic production of key technologies, boost its research and innovation, and secure its cyber infrastructure to ensure that foreign cyberattacks do not disrupt its goals [4]. By strengthening cybersecurity, increasing collaboration with trusted

international partners, and investing in research and development (R&D), China can reduce its vulnerabilities and strengthen its technological independence [4]. This provides China with the opportunity to push for self-reliance and decrease its dependency on foreign entities.

Reducing Dependency on Foreign Tech:

China has a long history of excluding U.S technology companies and products, specifically news media outlets and social media platforms such as Facebook and YouTube, over censorship concerns [2]. In the past, China's efforts to reduce its use of Western IT proceeded slowly, but Beijing has intensified the campaign in recent years [2]. In 2022, the Chinese government issued an order for state-owned companies in critical sectors to replace non-Chinese software on their networks by the end of 2027 [2]. China has also targeted U.S chipmakers– in 2023, it restricted the use of Micron chips from domestic infrastructure networks [2]. Furthermore, China has taken broader measures to address security risks that limit the flow of Chinese data internationally [2]. The government's push for stricter data security laws is a part of the broader strategy to ensure sensitive information remains under national control [2].

Policy Recommendation: Strengthening China's Technological Independence:

Made In China 2025(MIC 2025)

In 2015, Prime Minister LI Keqiang launched *Made in China 2025*, an initiative that strives to secure China's position as a global powerhouse in high-tech industries [6]. This ten-year strategy focuses on intelligent manufacturing in ten strategic sectors and aims to secure China's position as a global superpower in high-tech industries [6]. This plan is crucial for China's growth and competitiveness in the upcoming decades [6]. The following recommendations outline steps the

Chinese government should take to protect its digital infrastructure and achieve many of the goals in *Made in China 2025* [6].

1. **Strengthen Domestic Technological Development:** China should expand investments in its domestic research and development of critical technologies, especially in sectors that are targeted by sanctions and cyberattacks [6]. This includes semiconductors, AI, aerospace, telecommunications, and other high-end manufacturing [6]. Reducing reliance on foreign technologies involves creating and developing companies that innovate through research and development, dominate domestically, and produce competitive exports [6].
2. **Build a U.S.-China Agenda on Cybersecurity:** This suggestion is challenging, but not impossible, because any agenda must be realistic [1]. The agenda must accept that China and the United States have two significantly different viewpoints concerning the freedom of information on the web [1]. It also must respect the reality that a variety of nongovernmental actors play significant roles in each country's concerns about cybersecurity [1].
3. **Developing China's Cyber Workforce:** China must invest in next-generation cybersecurity technologies and develop a stronger cybersecurity workforce [3]. The CSIS claims that, "Chinese leadership is building the most extensive governance regime for cyberspace and information and communications technology (ICT) of any country in the world" [3]. However, this is only possible if China expands cybersecurity education programs to allow young professionals to gain more experience in the field [3]. Ultimately, China is already ahead of the United States, which has no national-level data

protection position, but they must continue to train cybersecurity professionals to remain in the lead [3].

References

1. Brookings Institution. (2012, February). *Cybersecurity and U.S.-China relations*. https://www.brookings.edu/wp-content/uploads/2016/06/0223_cybersecurity_china_us_lieberthal_singer_pdf_english.pdf
2. Carnegie Endowment for International Peace. (n.d.). *U.S.-China data regulation: Charting a path forward*. https://carnegie-production-assets.s3.amazonaws.com/static/files/Harrell_US-China%20Data%20Regulation.pdf
3. Center for Strategic and International Studies (CSIS). (n.d.). *China's emerging cyber governance system*. https://www.csis.org/programs/strategic-technologies-program/resources/china-cyber-outlook/chinas-emerging-cyber
4. China Briefing. (2024, January 2). *China issues new regulations on network data security management, effective January 1, 2025*. https://www.china-briefing.com/news/china-issues-new-regulations-on-network-data-security-management-effective-january-1-2025/?utm_source=chatgpt.com
5. Cyber Security Intelligence. (2023, May 10). *China complains about U.S. cyber attacks*. https://www.cybersecurityintelligence.com/blog/china-complains-about-us-cyber-attacks-8158.html
6. Institute for Security and Development Policy. (2018, June). *Made in China 2025: Backgrounder*. https://www.isdp.eu/wp-content/uploads/2018/06/Made-in-China-Backgrounder.pdf

7. National Security Institute. (2023). *The national security threat of Chinese technological innovation*. https://nationalsecurity.gmu.edu/wp-content/uploads/2023/08/The-National-Security-Threat-of-Chinese-Technological-Innovation.pdf
8. Office of the United States Trade Representative (USTR). (2018, June). *Section 301 investigation fact sheet*. https://ustr.gov/about-us/policy-offices/press-office/fact-sheets/2018/june/section-301-investigation-fact-sheet