Name: Brandon Harris

Date 3/25/2025

CYSE 426: Cyber War

Term: Spring 2025

Old Dominion University

Introduction

As Tensions between the United States and China have intensified in recent years, particularly over Taiwan, and as China seeks to assert dominance in the Indo-Pacific region, this has made the Chinese threat the top priority for the U.S. Department of Defense and the intelligence community. Among these threats, state-sponsored cyber operations by the People's Republic of China represent one of the most pressing issues for the United States. The Chinese government, through entities like the People's Liberation Army (PLA), the Ministry of State Security (MSS), and state-backed hacking groups, has continuously targeted U.S. government agencies, critical infrastructure, and private sector companies to gain economic, military, and strategic advantages over the United States. China's increasing focus on cyber operations that relate to intelligence gathering, the disruption of U.S. military operations, and preemptive strikes on critical infrastructure has made it a formidable adversary in the cyber domain. China's cyber operation teams also steal intellectual property and research and development data on the latest U.S. weapons and technology and create influence operations aimed at undermining U.S. interests. These persistent activities bring me concerns about the resilience of U.S. cybersecurity defenses and the long-term impact on national security. This growing threat not only concerns me the most but also shows why I believe the United States needs to invest in enhanced cyber defenses, strategic countermeasures, and take a more proactive approach to safeguarding the United States and countering China's expanding cyber warfare capabilities.

Threat assessment

China’s state-sponsored cyber activities against the United States are among the most persistent and advanced in the world, posing a direct threat to national security and the interests of the United States. Chinese threat actors use a wide range of tactics, techniques, and procedures (TTPs) to infiltrate sensitive U.S. networks, steal data, and position themselves for potential

cyber-enabled warfare. These operations are largely driven by the Ministry of State Security (MSS) and the People's Liberation Army (PLA), which oversee numerous Advanced Present Threat (APT) groups such as APT41, APT31, Mustang Panda, and Hafnium. These groups are who China employs to conduct cyber operations and are responsible for espionage, stealing new technology, and cyber operations designed to compromise the United States' critical infrastructure such as power, water, and transportation facilities. These advanced persistent threats use backdoors to maintain long-term access to compromised systems and sophisticated malware to cover their tracks and exfiltrate data quietly from networks. The U.S. Cybersecurity and Infrastructure Security Agency (CISA) has warned both public and private sectors about China's ability to infiltrate and lay dormant in secure networks by exploiting known and unknown vulnerabilities. Notably, in 2021, the Hafnium group, which is linked to the MSS, exploited vulnerabilities in Microsoft Exchange servers, allowing them to exfiltrate confidential emails and install web shells for continued access to the email servers (Mitigate Microsoft Exchange Server Vulnerabilities, CISA, 2021). These types of attacks show China's commitment to long term cyber campaigns, where they establish footholds within critical systems to extract valuable intelligence over extended periods.

China has also engaged in cyber operations for economic espionage, targeting key U.S. industries such as aerospace, defense, and pharmaceuticals. APT41, also known as Wicked Panda, a notorious Chinese hacking group, has been linked to widespread intellectual property theft, including the hacking of U.S. biotech firms to steal COVID-19 vaccine research and data (Two Chinese Hackers Working with the Ministry of State Security Charged with Global Computer Intrusion Campaign Targeting Intellectual Property and Confidential Business

Information, Including COVID-19 Research, U.S. Department of Justice, 2020). These intrusions are not for intelligence-gathering but serve China's broader strategic ambitions to achieve technological superiority over the United States. Alarmingly, China's cyber operations have shifted toward pre-positioning malware and establishing presistences within U.S. critical infrastructure. For example, the recent Volt Typhoon campaign, which was uncovered in 2023, revealed that Chinese threat actors had compromised U.S. power grids, water treatment plants, and telecommunications networks. Incident response investigations and digital forensics of the compromised systems and found that China had installed command and control channels and covert backdoors that could be activated in the event of a geopolitical crisis, such as a Chinese invasion of Taiwan (PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure, CISA & NSA, 2024). These intrusions indicate China's intent to damage or destroy U.S. infrastructure to make the United States vulnerable and to delay conventional military action and cause chaos domestically. Chinese threat actors also use living-off-the-land techniques, which means the malicious actors use native system processes and tools, such as PowerShell or network and management tools within the command line, to avoid detection. By blending in with normal network activity, groups like Mustang Panda have been able to conduct long-term reconnaissance on U.S. government agency networks.

China also uses influence operations by creating disinformation and misinformation to shape public perception and divide Americans along partisan lines. The MSS has been linked to coordinated disinformation campaigns on social media platforms, spreading divisive narratives about U.S. foreign policy, elections, and military actions in the Pacific. This hybrid warfare strategy works to erode trust in democratic institutions and shift public opinion in China's favor, which would complicate U.S. efforts to counter Beijing's strategic ambitions and potentially help

to prevent a response to an invasion of Taiwan. China's cyber capabilities continue to evolve, with emerging threats that blend artificial intelligence and quantum computing and malware that is becoming better at hiding within compromised systems. With a larger pool of cyber personnel, China can dedicate tens of thousands of hackers to targeting U.S. networks, while the United States has far fewer hands on keyboards that can actively conduct cyber operations against China. The persistent and methodical nature of its cyber operations shows that China is preparing for a conventional conflict with a near-peer nation. As tensions over Taiwan escalate, the risk of cyber warfare between China and the United States grows every day, making it essential for national security agencies to remain vigilant against China's expanding influence and cyber capabilities.

Implications for U.S. national security

The implications of China's cyber operations for U.S. national security are far-reaching. At the strategic level, these operations are eroding U.S. military superiority by allowing Chinese intelligence operatives access to military technologies, defense systems, and operational plans. The theft of classified data related to U.S. defense contractors has already enabled the rapid advancement of China's military capabilities, narrowing the technological gap between the two nations. If left unchecked, China's cyber campaign could continue to undermine U.S. defense readiness, allowing the PLA to counteract and even match the U.S. military's weapons and strategies on the battlefield. China's operations also pose a direct threat to U.S. military logistics and readiness. Constant access to command and control systems that involve the movement of troops and equipment and satellite communications provides Chinese threat actors with the capability to degrade and disrupt military operations at key moments. In the event of a military conflict, In a scenario involving Taiwan, China could use its foothold in critical networks to

delay U.S. force deployment and make the battlefield turn disfavorably for the United States. This type of asymmetric warfare could neutralize U.S. advantages in conventional military power, forcing the United States to fight in a contested cyber domain where infrastructure disruptions hinder operational effectiveness. As China continues to advance its cyber warfare capabilities, the United States must grapple with the reality that cyber threats are no longer just tools used for espionage but a weapon used for war. The growing sophistication of China's cyber arsenal increases the risk of destructive cyber operations that could neutralize key military assets, and cripple national infrastructure in the event of a geopolitical conflict.

Beyond military concerns, one of the most concerning aspects of this cyber-enabled theft is its long-term impact on U.S. industry. American companies spend years and billions of dollars researching and developing groundbreaking technologies only to have them stolen from them and then replicated by Chinese organizations with state backing. This not only weakens the financial standing of U.S. businesses but also discourages future investments in new technologies as companies fear their innovations may be stolen with little consequence. The loss of proprietary knowledge lets Chinese competitors flood the global market with cheaper alternatives, putting U.S. firms at a disadvantage. China's cyber theft also threatens U.S. infrastructure tied to economic stability. Cyber operations targeting Banking institutions, supply chain networks, and transportation systems disrupt trade and manipulate financial markets. A coordinated cyber attack on the U.S. banking sector, for example, could disrupt financial transactions and cause Americans to lose money. China's ability to embed itself into U.S. critical infrastructure, such as energy grids or telecommunications networks, is the most alarming, as vulnerabilities in U.S. critical infrastructure have given China's hackers access to the United

States' nuclear power plants, water treatment facilities, and emergency services, presenting a grave risk to the United States. In a worst-case scenario, a coordinated cyber attack by Chinese state-sponsored actors could cripple vital services, resulting in widespread panic, and potential loss of life. The ability to remotely disable power plants or information systems such as emergency broadcasts could be leveraged against the United States or even lead to kinetic military action. Given the severity of these threats, the United States must take decisive action to get ahead of this threat, deter Chinese cyber aggression, and mitigate potential risks. The question remains: What can be done to stop and mitigate these growing cyber threats? Tackling this issue demands a comprehensive strategy that should include hiring more workers, improving the skills of the current workforce, and working with our allies to go after these threats together.

What can be done

As China continues to improve and unleash its cyber capabilities, the United States must confront China’s aggression not just in networks but also by countering state-sponsored cyber threats through stronger defenses, strategic deterrence, and international cooperation. Strengthening national cybersecurity requires a complex approach that upgrades not only current defenses but also invests in future ones. The U.S. government, private sector, and allied nations must work together to thwart China’s intrusions and prevent long-term damage to national security, the global economy, and military readiness. An immediate step the United States can take to enhance its cyber defense posture is sharing intelligence and exposing China's state-sponsored hacking groups' tools and tactics. Doing this can expose current operations and allow defenses to be created to make China's cyber operations more costly to conduct. Federal agencies such as the Cybersecurity and Infrastructure Security Agency, the National Security Agency, and U.S. Cyber Command must expand their capabilities to detect, analyze, and respond to cyber threats originating from China. This can look like hiring and training more skilled workers to identify and neutralize threats before they can cause significant

harm and alerting the public on what to look out for if they are in a sector that Chinese threat actors are currently targeting. Expanding collaboration between the public and private sectors can help improve the rapid sharing of cyber threat intelligence and assist both government and industry stay on the forefront with up-to-date information on emerging threats coming from China.

Protecting critical infrastructure is another crucial part of countering China's cyber threat. The U.S. must implement stricter cybersecurity standards for private sector organizations that own and operate critical infrastructure, which has been a favorite target of the Chinese. The federal government should enforce existing policy by fining organizations who are in violation of government cybersecurity policy and consider legal action against operators who carelessness can cause a major data breach. Another area that needs more security is the United States supply chain, as Chinese threat actors have demonstrated a capacity to compromise hardware and software used in U.S. systems. The U.S. must reduce its reliance on Chinese-manufactured technology and components to mitigate supply chain vulnerabilities, particularly in the telecommunications and semiconductor industries. Investing in domestic semiconductor production through legislation and even tax breaks for corporations will help decrease dependence on foreign suppliers and protect against hardware-level cyber threats. Also, implementing stricter vetting processes for foreign companies operating in the U.S. will prevent adversaries from embedding backdoors and malware into American infrastructure. The United States should also be more aggressive with offensive cyber operations, The U.S. must strengthen and restore deterrence by showing China we can impose more pain on them than they can on us should they choose to escalate to conflict. Being more aggressive does not just include cyber operations but also increasing the use of targeted sanctions against individuals and organizations affiliated with the Chinese government's cyber operations. The Department of Justice and the

FBI should also continue using all legal means against Chinese cybercriminals, indicting known hackers and exposing their activities to limit their operational effectiveness. U.S. Cyber Command should be using its resources to destroy China's command and control infrastructure, find and destroy any deployed malware, and actively disrupt Chinese cyber operations before they can escalate into more severe threats.

International partnerships will also be important in countering China’s cyber threat. Utilizing NATO, the Five Eyes intelligence-sharing network, and Indo-Pacific partners such as Japan, Australia, and South Korea while conducting joint cybersecurity exercises, sharing intelligence, and coordinating responses to cyber incidents will create a unified front and will help the U.S. build a collective defense against China's cyber operations. Also, advocating for international norms and agreements on responsible state behavior in cyberspace can help pressure China to stop its cyber activities.

Conculsion

China’s state-sponsored cyber operations present one of the most significant threats to U.S. national security, targeting military systems, critical infrastructure, and the private sector. China has undermined U.S. technological superiority and has also worked to jeopardize our economy and military readiness. As China continues to expand its cyber warfare capabilities, the United States must take a more active approach to counter these threats. Failure to do so will leave the nation vulnerable to large-scale disruptions and an unwinnable conflict. The United States has to make a comprehensive strategy that will deter the Chinese cyber threat. To strengthen the United States' cybersecurity, it should invest in the workforce, improve critical infrastructure protections, and give federal agencies such as CISA, NSA, and U.S. Cyber Command the ability to use and create new capabilities to expose and neutralize Chinese threat actors before they can

cause serious damage. Increasing collaboration between the government and the private sector will allow for rapid dissemination of information related to emerging cyber threats that originate from China, enabling organizations to implement stronger defenses.

The United States should reduce its reliance on Chinese-manufactured technology and secure the U.S. supply chain to prevent catastrophic vulnerabilities that adversaries could exploit. Implementing stricter cybersecurity regulations for critical industries and holding organizations accountable for negligence in safeguarding sensitive data will further reinforce national security. The United States must also use its offensive cyber capabilities to impose real consequences on Chinese actors engaged in malicious cyber activities, creating deterrence through targeted sanctions and legal action against identified threat actors. As cyber warfare becomes an increasingly critical domain of conflict, the U.S. must act decisively to counter China's growing confidence in cyberspace. Only through strategic investments, strong partnerships, and a proactive defense posture can the nation safeguard its security, economy, and technological leadership in the face of an evolving enemy.

References

CISA, C. (2021, July 19). *Mitigate microsoft exchange server vulnerabilities: CISA*. Cybersecurity and Infrastructure Security Agency CISA. https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-062a

CISA, C. (2025, February 7). *PRC state-sponsored actors compromise and maintain persistent access to U.S. critical infrastructure: CISA*. Cybersecurity and Infrastructure Security Agency CISA. https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a

DOJ, D. (2025, February 6). *Two Chinese hackers working with the Ministry of State Security charged with global computer intrusion campaign targeting intellectual property and confidential business information, including COVID-19 Research*. Office of Public Affairs | Two Chinese Hackers Working with the Ministry of State Security Charged with Global Computer Intrusion Campaign Targeting Intellectual Property and Confidential Business Information, Including COVID-19 Research | United States Department of Justice.https://www.justice.gov/archives/opa/pr/two-chinese-hackers-working-ministry-state-security-charged-global-computer-intrusion

Goldsmith, J. (Ed.). (2022). *The United States' Defend Forward Cyber Strategy: A Comprehensive Legal Assessment*. Oxford University Press.https://books.google.com/books?hl=en&lr=&id=nHhXEAAAQBAJ&oi=fnd&pg=PP1&dq=the+United+states+countering+china+cyber+operations&ots=hv1vg2isep&sig=ApaCGoAcvfltdLhqPuu7fuUkgcQ

Hjortdal, M. (2011). China's use of cyber warfare: Espionage meets strategic deterrence. *Journal of Strategic Security*, *4*(2), 1-24.https://www.jstor.org/stable/26463924

Krekel, B., Adams, P., & Bakos, G. (2014). Occupying the information high ground: Chinese capabilities for computer network operations and cyber espionage. *International Journal of Computer Research*, *21*(4),333.https://search.proquest.com/openview/538928e19733a945f802fdb5b49518f7/1?pq-origsite=gscholar&cbl=2034869&casa_token=1iRh8U5F7zEAAAAA:liwIwQxx6Ftg28Y0bOls8vDaRDvxK1vtcUKoWVLcDOLHOdUnnddKCfUhgzXWOcK_DNusvfEJFZw

Segal, A. (2016). US Offensive Cyber Operations in a China-US Military Confrontation. *Available at SSRN 2836203*.https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2836203

Smeets, M. (2018). The strategic promise of offensive cyber operations. *Strategic Studies Quarterly*, *12*(3), 90-113.https://www.jstor.org/stable/26481911

Stokes, M. A., & Hsiao, L. R. (2012). *Countering Chinese cyber operations: Opportunities and challenges for US interests*. Project 2049 Institute.https://nsarchive.gwu.edu/sites/default/files/documents/2700166/Document-79.pdf